A Security Solution for Bank Card

Xiang-Yi HU\textsuperscript{1,a}, Gui-Fen ZHAO\textsuperscript{2,b}, Yan-Jiao MA\textsuperscript{3,c}

\textsuperscript{1}Beijing Key Laboratory of Network Cryptography Authentication, Beijing, China
\textsuperscript{2}Beijing Municipal Institute of Science & Technology Information, Beijing Key Laboratory of Network Cryptography Authentication, Beijing, China
\textsuperscript{3}Datang Liancheng Information System Technology Co., Ltd., Beijing, China

\textsuperscript{a}huxy368@sohu.com, \textsuperscript{b}gfzh@hotmail.com
*Corresponding author

Keywords: Magnetic Stripe Bank Cards, Memory Chip Bank Card, CPU Chip Bank Card, Withdraw Money Password, Digital Signature and Encryption, Vertical Authentication, Combined Secret Key, PKI.

Abstract. Analyze the management vulnerabilities and technology vulnerabilities of current bank cards firstly, explain the technical features of the magnetic stripe and memory chip bank card, and disclose the method probably used by criminals while attacking. Meanwhile analyze the reasons why PKI may be infeasible to guarantee the security of bank cards. Vertical authentication based security solution for bank cards are proposed. Use CPU smart chip to replace the magnetic stripe card and memory chip. Set up signature and encryption protocols dealing with withdrawal form or payment order on the basis of vertical authentication in CPU smart chips, and replace current withdrawal or payment password authentication protocol. Therefore, set up a chip-level withdrawal or payment system for ATM or POS to guarantee the security of bank card withdrawal or payment.

Introduction

Current bank cards are used nearly 30 years. Some bank card user funds stolen events have occurred frequently and been reported in these years. The bank cards in these events are magnetic stripe cards. User information is written in the magnetic stripe and easily read and copied. User information is sold by criminals over network. Criminal group purchase, or use the card reader to read, or steal the user's account and password in mobile phone by virus. And then copy user bank cards, steal funds on ATM using the stolen password, or pay via POS. User's funds losses are caused (show as Fig.1), which also harm the country's financial security.

Figure 1. Fraudulent Bank Cards.
In recent years, banks upgrade bank card security, provide bank card with a memory chip one after another for users. Bank card with memory chip use lower price memory chip, the user's personal information and the withdrawal or payment password are stored in the memory chip. Memory chips can prevent criminals reading user information by card reader. But memory chip bank card only adopts fixed withdrawal or payment password authentication with lower security level, to realize payment via the ATM or POS, there are also security vulnerabilities as magnetic stripe bank card. For example: criminals can obtain the user's personal information and the withdrawal or payment password through online purchase or by virus program, to clone the memory chip of the bank card, and then steal user account funds.

For solving the security problems of bank cards, we propose CPU chip solution to replace current magnetic stripe bank cards and memory chip bank card. Set up withdraw money or payment order signature and encryption protocol in CPU chip to achieve technical update for bank card security system. If use signature and encryption technology based on PKI to update bank card security system, although it is feasible, it could not achieve in fact. Because the amount of bank cards is about 100 times of network users, the PKI run slowly and could not meet the requirement of large-scale bank cards concurrent authentication. Consequently, we propose authentication method based on vertical authentication for bank card security update. Vertical authentication means key seeds are generated, written, distributed and destroyed in a concentrated way, and adopt symmetric encryption algorithm (SM1 or SM4) and combined key generation algorithm to build trusted bank card withdraw or payment protocol on the basis of digital signature and encryption (SM4). The concurrent signature verification speed is 200 times than PKI. It could solve the current problems of bank card user funds stolen caused by the information leakage.

**Security Analysis of Magnetic Stripe Bank Cards and Memory Chip Bank Cards**

**Security Analysis of Magnetic Stripe Bank Cards**

Magnetic stripe bank cards store the user's personal information, including account name, identity card number, bank where opened the account, account number, withdrawal or payment password, etc. in magnetic stripe. Magnetic stripe card data can be illegally readout, criminal gangs through online purchase, or using card reader read, or through a virus to steal the bank card user information and withdrawal key (password) in user's mobile phone and cloned the user's bank card, thus, steal the user's bank account funds. Magnetic stripe bank cards is an early product, the security level is low. As early as 10 years ago, the founder of the Microsoft Corp Bill Gates asserted: if the bank card does not upgrade into a chip card10 years later, the security of the bank card will be disastrous.

**Security Analysis of Memory Chip Bank Cards**

By using the memory chip production of bank cards, the user's personal information, including account name, identity card number, bank where opened the account, account number, withdrawal or payment password, is stored in a memory chip of a bank card. Storage chip can prevent criminals using the reader to steal user information. However, the memory chip bank card uses a fixed withdrawal or payment password for authentication. Anyone can withdraw money from the ATM or payment via POS after passing the password authentication. There is the same security vulnerabilities compared with the magnetic stripe bank card, such as: criminals can through the online purchase, or by virus program to obtain the user's personal information and the withdrawal or payment password, to clone with a memory chip of the bank card, and steal the user accounts funds.

**Update Current Bank Cards with CPU Smart Card**

Distribute a new bank card with CPU chip for each bank user. Regard the CPU bank card as the main card, and the other bank cards issued before by bank as deputy cards.
Bind all Bank Accounts with CPU Bank Card

Bind CPU smart card with the user's identity one by one (to save the cost of smart cards with CPU chips, Union Pay can coordinate all banks issued a bank card with CPU chip to each bank user). A bank card with a CPU chip corresponds to a number of accounts in the bank (see Figure 3), i.e., the bank card with CPU chip is bound to all the bank's accounts (a user may open multiple accounts at a bank). CPU chip bank card can achieve large (3000 RMB or more) withdrawals in the ATM, or large (3000 RMB or more) payment on the POS. The bound (a magnetic stripe or a memory chip) bank cards can only query bank card balance, small (3000 RMB or less) withdrawal and payment, the bank staff perform large withdrawals or transfers etc. for users if on the counter of the bank.

CPU Bank Card and Encryption System can Prevent Clone of Bank Cards

In CPU card chip bank cards, using PKI or IBE technology establish withdrawal or payment protocol, is perform encryption and signature for the withdrawal or payment order. Criminals can’t clone bank card with CPU chip, can’t access to the user's private key, also can’t tamper with the content of withdraw or payment order, which insure user account funds security with CPU bank card.

Low Efficiency of Withdraw or Payment Protocol Based on PKI or IBE

The characteristic of PKI or IBE based signature and encryption protocol is that two cryptosystems, i.e. symmetric cipher algorithm and asymmetric cipher algorithm, are adopted simultaneously to establish digital signature and encryption protocol, which call asymmetric cipher algorithm twice and call three keys. So the security architecture is complex, there are more procedures during signature and encryption. The efficiency of signature and encryption protocol is low. If use PKI or IBE technology for updating security system for bank cards, although it is feasible, it could not achieve in fact. Because the amount of bank cards is about 100 times of network users, the PKI or IBE run slowly and could not meet the requirement of large-scale bank cards concurrent authentication. Moreover, the cost of CA is higher, it is hard to pay the construction cost of CA. Thus, PKI and IBE based signature and encryption protocol can’t be favored by the security update for bank cards.

Authentication, Withdraw or Payment Protocols Based on Vertical Authentication

Establish authentication, signature and encryption protocol based on vertical authentication, i.e. symmetric cipher algorithm (SM1 or SM4), hash algorithm (SM3), combined secret key generation algorithm, authentication protocol, signature and encryption protocols, key seeds, withdraw or payment password, user’s identity card number are written into user’s bank card with CPU smart card. Users’ key seeds are different from each other.

Vertical authentication adopts symmetric cipher algorithm and combined secret key algorithm to establish authentication, signature and encryption protocols. Combined secret key generation algorithm solves the problem of secret key update and management. Key seeds are generated, written, distributed and destroyed centrally [1].

Authentication Protocol at Bank Card

User plunged in bank card with CPU chip into the ATM or POS, after the device prompts, users enter the withdrawal or payment password, and press the “confirm” button. Encryption system at CPU bank card with intelligent chip generate a set of key generation parameters, generate a set of symmetric keys according to the combined secret key generation algorithm based on vertical authentication mode, and combine the withdraw or payment password input by user (with logical AND or XOR) to generate authentication key, then generate the authentication password 1, and send the user identity card number, key generation parameters and authentication password 1 to the authentication center. Encryption system at authentication center generate a set of symmetric keys
according to the key generation parameter and key generation algorithm, and combine the user's withdrawal or payment password to generated the authentication key, and then generate the authentication password 2, by comparing the authentication password 1 and 2 is the same or not, to confirm the identity of the user is trusted or not.

After authentication by authentication center for CPU bank card user, bank payment platform return authentication result to ATM or POS and show all bank account of the verified card user (a user may open multiple accounts in the same bank) and account fund balance. If user failed to pass the authentication, the ATM or POS shows key or password error of the CPU bank card.

**Signature and Encryption Protocol at Bank Card**

User click the withdraw or payment button, and press the “confirm” button. Encryption system at CPU bank card with intelligent chip generate a set of symmetric keys according to the combination secret key generation algorithm, and combine the withdraw or payment password input by user (with logical AND or XOR) to generate signature and encryption key, and then perform signature and encryption for withdraw or payment order including amount, identity card number, user account number, account number, etc. using symmetric cipher algorithm (SM1 or SM4), hash algorithm (SM3). ATM or POS send the cipher text and digital signature of withdraw or payment order, and key generation parameters to authentication center of bank payment system.

**Signature Verification and Decryption Protocol at Bank Card**

Encryption system at authentication center generate a set of symmetric keys according to the received key generation parameters and combination secret key generation algorithm, and combine the withdraw or payment password to generate signature verification and decryption key, and then perform decryption and signature verification (integrity verification) for the cipher text of withdraw or payment order.

If the withdraw or payment order pass the verification, bank payment system send withdraw instructions to ATM or send payment instructions to POS. If the withdraw or payment order can’t pass the verification, bank payment system send password error to ATM for preventing withdraw, or to POS for preventing payment.

**High Efficiency and Low Cost of Vertical Authentication**

Encryption system at authentication center generate a set of symmetric keys according to the received key generation parameters and combination secret key generation algorithm, and combine the withdraw or payment password to generate signature verification and decryption key, and then perform decryption and signature verification (integrity verification) for the cipher text of withdraw or payment order.

Vertical authentication based authentication, encryption and signature protocol only adopt SM1 or SM4 algorithm to build authentication, signature and encryption protocol. The security architecture is simple, and calls only one key to perform encryption and signature of payment order. There are less procedures during signature and encryption, thus the efficiency is higher. There is a common sense in some books: symmetric cipher algorithm runs faster 100 times than asymmetric cipher algorithm in computer internal memory, and runs faster 1000 times in CMOS chip [9]. Consequently, authentication, encryption and signature protocol based on vertical authentication owns the advantages of high security, high speed and low cost, which could provide security technology support for bank card upgrade for CPU chip card.

**Security Analysis of Bank Card Upgrade Solution**

The CPU smart chip replaces the current use of magnetic stripe and memory chip to upgrade bank card. Establish CPU chip bank cards based encryption system and authentication protocol, signature and encryption protocols. Combine withdraw or payment password input in the ATM or POS by user with a set of symmetric keys according to the combined secret key generation algorithm (with
logical AND or XOR) to generate authentication key, signature and encryption key. After authentication, user access user account and the account balance. Through the signature and encryption protocol, users realize withdrawals from the ATM, or on pay via POS. At the same time, users still enter the withdrawal password during the process of withdrawal or payment to achieve the same operating process and the operating habits of user withdrawals or payment.

Even if hackers gain access to the user's withdrawal or payment password, since the CPU bank card encryption system can’t be cloned, hackers are unable to get one-time authentication key, signature and encryption key in CPU chip bank card. Therefore, hackers cannot steal the user's bank card funds (as Fig. 2). Thus, ensure the safety of the bank card system.

![Figure 2. Hackers can’t Clone CPU Bank Cards.](image)

**Things that Need the Cooperation of the Bank**

**Deployment of Authentication Center in the Bank's Computer Room**

Deploy authentication center based on vertical authentication mode in the bank's computer room, including key management server, authentication and signature verification server, etc. And combine it with the authority management system of bank payment platform (shown as Fig. 3). There is only decryption and signature verification protocol in authentication center, all users’ key seeds are stored after encryption, decryption key for decrypting key seeds is stored in the encryption chip of hardware device.
Update of Bank Card Software System

The bank is responsible for the development of the software interface between ATM or POS and the CPU intelligent chip bank card, which can be inserted into the ATM or POS (shown as Fig. 4).

Bind User’s CPU Chip Bank Card with the user’s Multiple Account

Bank is responsible for binding user's CPU chip bank card with the user's multiple account numbers in corresponding bank (a user might open multiple accounts in a bank), namely, a CPU bank card correspond to multi magnetic stripe or a storage chip bank card and account numbers (shown as Fig. 5).
Interface Development

The bank is responsible for interface development between the authentication center and the bank payment platform, the bank provides the authority management system interface of bank payment platform to integrate with authentication center based on the "vertical authentication". The bank payment platform received authentication protocol, or signature and encryption protocol data from ATM or POS terminal, and then transmitted to the authentication center. Authentication center returned the authentication results or signature verification results to bank payment platform. If pass authentication, bank payment platform feedback all the users’ corresponding bank accounts and the fund balance to the ATM or POS terminal, otherwise the ATM or POS terminal display bank card withdraw or pay password error. If pass the signature verification (integrity verification of withdraw or payment order), bank payment platform send withdraw instructions to the ATM, or sent the payment instructions to POS. Otherwise, ATM or POS terminal display bank card password error.

Summary

Anyway, bank provide users bank card with CPU chip, bind user's CPU chip bank card with the user's multiple bank cards (magnetic stripe or a storage chip bank card) in corresponding bank. Regard the CPU bank card as the main card which achieve large (3000 RMB or more) withdrawals in the ATM, or large (3000 RMB or more) payment on the POS. Regard the other bank cards issued before by bank as deputy cards which can only query bank card balance, small (3000 RMB or less) withdrawal and payment, the bank staff perform large withdrawals or transfers etc. for users if on the counter of the bank.

Adopt vertical authentication method in CPU chip bank card, i.e. adopt symmetric encryption algorithm (SM1 or SM4) and HASH algorithm (SM3) to build authentication, signature and encryption protocol, perform authentication for bank card users, and signature and encryption for withdraw or payment orders. Using the combined secret key generation algorithm to solve the problem of secret key management, ensure the one-time authentication key, signature and encryption key. And authentication protocol, signature and encryption protocol runs in the CPU smart chips (such as the smart chip in U aegis), which is the chip level authentication, signature and encryption protocols with the advantage of higher security level. Criminals can’t clone CPU bank card and its encryption system, so they can’t get the one-time authentication, signature and encryption keys. In
addition, contrasted with international third party certification mode (e.g. PKI or IBE), vertical authentication mode improve the speed of concurrent authentication 100 times, increased the speed of the concurrent signature verification by 200 times, reduce the construction cost of the authentication center by 80 ~ 90%. Therefore, we propose a bank card security solution, to solve the security problem of the magnetic stripe bank card and the memory chip bank card.

At the same time, in the bank card security solution, ATM or POS and other hardware equipments are unchanged, mainly to upgrade its software system. The magnetic stripe or memory chip bank card are replaced by CPU bank card (such as the smart chip in U aegis), the banks invested less funds can complete upgrade of bank card security system. Thus, solve the problem of bank card security, which has attracted the attention of the society, and ensure the security of the national financial system.

Acknowledgement
This research was supported by Beijing Key Laboratory of Network Cryptography Authentication.

References