INFORMATION SECURITY

PAYMENT CARDS COUNTERFEITING METHODS AND PIN UNCOVERING

Goran Kunjadić[1],
Mladen Veinović[1],
Milan M. Milosavljević[1]

[1]Singidunum University,
Belgrade, Serbia

Abstract:

The problem of counterfeiting payment cards represents a significant issue for banks. So far, attackers have successfully forged cards with a magnetic stripe while no chip card has been counterfeited yet. On magnetic stripe cards Personal Identification Number - PIN value is not successfully reconstructed, thus limiting the use of counterfeit cards, while on the card with a chip attackers try programming the chip to give an affirmative answer to every request. The goal of this paper is to show that it is possible to discover the PIN value from the data on the magnetic stripe and thus compromise the chip itself if it is a card with a chip. Taking into account the results of this work a bank should become aware of the vulnerability of cards and discuss new methods of protection.

Keywords:

forging, cryptanalysis, payment security.

1. INTRODUCTION

In this paper, we want to draw attention of bankers as well as the general public to the potential vulnerability of the payment cards with microprocessor. While considering the payment card issues it is good to have on mind that over 90% of world money is digitalized [1]. It means that money becomes a data record in database and that with one simple key press on "delete" button someone can lose a significant amount of money [2]. Non-cash payments are widely accepted so the risk of misuse of payment cards becomes increasingly common. Counterfeiting the cards that have only magnetic stripe is trivial while making a copy of card that contains microprocessor is not yet successful despite numerous attempts. Counterfeit card can be easily used for online payment, whether the PIN is revealed or not. The necessary information is easy to access on the magnetic stripe. Using the card on the Automatic Teller Machine - ATM or Point Of Sale - POS [3] is most challenging as one has to know the PIN value which cannot be seen on the magnetic stripe like open text which is the issue for attacker. The PIN value cannot be revealed from the chip because of many reasons. The different manufacturer has different hardware configurations so it is not easy to discover the memory location of particular data without manufacturer documentation. Even with the

Correspondence:
Goran Kunjadić

e-mail:
gkunjadic@singidunum.ac.rs

DOI: 10.15308/Sinteza-2017-63-67

documentation, the encrypted PIN value is placed into the protected memory location. The fact which is neglected is that the PIN value is the same for one card, both on chip and magnetic stripe. Therefore, if someone revealed the PIN from the magnetic stripe it would be the same PIN, which is used for the chip. In that way the whole system of the chip card is broken.

2. PIN VERIFICATION METHOD

For the magnetic stripe card, the cardholder signature is the primary way to identify the person presenting a payment card. Verification is made by comparing the signature on the transaction draft to the signature on the card's signature panel. If two signatures match, there is a high probability that the cardholder's identity has been verified. Commonly available technologies support one widespread solution of cardholder identity verification and that is the PIN.

The verification process begins when the cardholder enters a PIN at an ATM keyboard or at a POS terminal. When the PIN is verified online, the PIN entered is encrypted, transmitted, decrypted and compared to a reference PIN available only in the issuer's processing center. The PIN can also be confirmed by using cryptographic transformation of the entered PIN that is compared against and identical cryptographic transformation of the reference PIN. If two versions of the PIN match, there is a high probability that cardholder's identity is verified. When the PIN is verified offline, the entered PIN is compared to the PIN stored on the card's chip. If two PINs match, then there is a high probability that the cardholder's identity has been verified.

The minimum PIN length is four digits. An issuer can elect to support longer PINs up to 12 digits. However, ATM acquirers are not obliged to support PINs of more than six digits. The PIN entered by the cardholder can consist of numeric digits 0 through 9, alphabetic characters A through Z, or combination of both. PINs are always numeric. The cardholder may use alpha to remember the PINs but PINs do not contain alpha characters [4]. When entering an alphabetic PIN character, the cardholder selects the key labeled with the corresponding alphabetic character. If the keys are not labeled with alphabetic characters, the cardholder selects appropriate numeric key after converting the alphabetic character to a numeric digit [5].

The value of PIN as a means of cardholder identification depends on the ability to ensure that the PIN is known only to the cardholder. Issuers should be assured that PINs would not be compromised when using them in other members' equipment or facilities.

A Pin Verification Service - PVS is provided by the issuer. This service compares the cardholder's PIN entry to a cryptographic transformation of that PIN. This technique is referred to as the PIN Verification Value - PVV method of verification [6].

The PVV method is a two-step process:

1. When a card is issued, the issuer derives a 4-digit PVV. The PVV and PIN Verification Key Index - PVKI are encoded on the magnetic stripe of the card or in online database. The stored PVV is called the reference PVV for comparison.
2. When a cardholder enters a PIN, a transaction PVV is generated. The transaction PVV is then compared to the reference PVV by the issuer's processing center. If two PVVs match, there is a high probability (9999 in 10.000) that the PIN is correct.

PVVs are four-digit decimal values. For any one PVV, there are only 10.000 possible combinations of digits. If an adversary has a method of trying all 10.000 PVV combinations on a single account, the adversary will discover the PIN, or an equivalent value that transforms to the same PVV.

It is not feasible to test all 10.000 combinations manually. However, it may be possible to obtain the information needed to perpetrate a fraud by using an automated method, such as inserting microcomputers in communication lines, creating spurious transactions, and recording authorization responses. Automated testing trials such as these would not expose the PIN Verification keys but could compromise an individual PIN/PAN - Primary Account Number combination. To detect such trials, the PIN Verification service monitors the entry of incorrect PINs and declines transactions when the maximum number of incorrect OINs has been entered.

The PVV method is based on the Data Encryption Standard - DES algorithm and pair of DES keys designated as a PIN Verification Key - PVK pair. The algorithm may be implemented in hardware or software within a tamper-resistant security module. Each issuer creates its own PVKs. These keys should be different from any other DES keys used by that issuer. Because each issuer has unique keys, a breach of security is limited to a particular issuer rather than to all issuers using PVV method [7], [8].

To create a PVV, the PVK pair is input to the DES algorithm together with other data. Like any DES-based scheme, the security depends on the secrecy of the DES keys. The PVK pair must be kept secret and should not

be known to anyone. If the unauthorized disclosure of a PVK pair is known or suspected, the PVK pair should be immediately replaced. Cards with PVVs generated using the potentially compromised key should be reissued as soon as possible, and when all such cards have been reissued, the potentially compromised PVK pair should be invalidated. To minimize the number of cards that should be reissued under this condition, it may be desirable to use a new PVK pair for each reissue.

3. DES KEY MANAGEMENT

The process of securely generating, distributing, and storing Data Encryption Standard keys is called Key Management. Key management procedures are supposed to be highly secure. The compromise of even a single key could lead to the compromise of all PINs encrypted under that key. A DES key has one of the following functions:

- A working key protects PINs and other data
- A Master key protects other keys
- Working keys are secret values that are input to the DES process. The following are examples of working keys:
- The keys needed to encrypt and decrypt PINs before and after message transmission or host storage.
- The pair of keys used to generate the PIN Verification Value.The pair of keys used to generate the Card Verification Value - CVV in Visa notation or Card Verification Code - CVC in MasterCard notation
- The pair of keys used to generate the Card authentication Verification Value - CAVV.

To obtain valid results, the same working key must be used both for encryption and for decryption. Likewise, to verify a PIN with the PVV or to validate a CVV, the original encryption keys are required [9].

Key Exchange Keys

Key Exchange Keys - KEK are used to protect, meaning encrypt and decrypt working keys so they can be safely stored or conveyed from one network node to another.

The Zone Control Master Key – ZCMK Z is a type of KEK. It is used to protect other keys during transit. It can be used to transfer keys between Hardware Security Modules - HSMs. Transferred keys are encrypted under ZCMK outside of HSM and generally transferred between HSMs in a 3-component form. Firstly, generate a ZMK key, Export ZMK in 3 components and send those components to other HSM with 3 different key officers. When key officers import those 3 components to other HSM you are ready to send keys to other HSM. Also, a member uses the ZCMK to encrypt working keys before sending them to Visa or MasterCard. The Visa or MasterCard uses the ZCMK to decrypt the working keys it receives. Before storing the member's keys, Visa or MasterCard encrypts the keys again under a particular key only known to them. Visa or MasterCard uses ZCMK to encrypt working keys before sending them to a member. A member uses the ZCMK to decrypt the working keys it receives [10].

Master keys

A member master key is used by a member to protect its keys for in-house storage. This key is known only within a physically secure device at the member's processing center. The most commonly using devices are HSMs. A member master key could be used to encrypt any of the working keys, KEKs or ZCMKs used in interchange processing. The same master key should not be used to encrypt both working keys and master keys.

Key Check Value

A key check value is a six-digit, hexadecimal value that is obtained by encrypting a block of zeroes under a given key. The first six digits of the resulting ciphertext present the key check value for that key. Some HSMs only return the first four digits. The key check value does not need to be protected since it cannot be used to backtrack to the cleartext key. Because the encryption of zeroes under the same key always generate the same results. The key check value can be used to verify that two copies of a key are in fact identical.

Dynamic Key Exchange - DKE Service

The Dynamic Key Exchange Service is an optional service that enables members to periodically change working keys used to protect cardholder PINs. These keys can be changed dynamically through the exchange of online messages. The Dynamic Key Exchange Service offers alternatives for key conveyance, both of which protect PINs from disclosure during transmission [11].

- The member sends an administrative request to Visa or MasterCard for a new acquirer or new issuer working key. After receiving the request, Visa or MasterCard generates the appropriate

working key and sends it online to the member.

- The member authorizes Visa or MasterCard to automatically generate new acquirer and new issuer working keys on a daily basis. The member may specify time and day when Visa or MasterCard should generate and send new keys before sending an authorization request to issuer.

Keys are exchanged using 0800 and 0810 network management messages [12].

Message Security Code - MSC is a part of the message with the purpose to confirm that the message comes from the stated sender and has not been changed [13].

Both acquirers and issuers should evaluate possible alternative processes if problems are encountered during the implementation. It is recommended that a procedure should be established to allow a return to manual key procedures. Europay, MasterCard and Visa – EMV offer the following two procedures:

- *Offline*

When a key problem is discovered, EMV will contact the member or the member will contact EMV and the further generation of working keys is temporary halted. When the Offline procedure is invoked, EMV will start using the static key in messages sent to the member. The operator at the member site must be familiar with the procedure for transferring their static keys to their dynamic key areas. The method for doing this will vary by member. Once this static key is in place, EMV will coordinate with the member to return to dynamics key.

- Fallback

When the Fallback option is used, EMV will send the member 0800 key exchange message in which the key in MSC is equal to zeros. When MSC is filled with zeros, the numbers should switch to their static keys and send 0810 response with Response Code Zero - MSC. If the member does not respond with an approval, system will not use the static key. This Fallback procedure is similar to the normal key exchange process, except that MSC contains zeros [14].

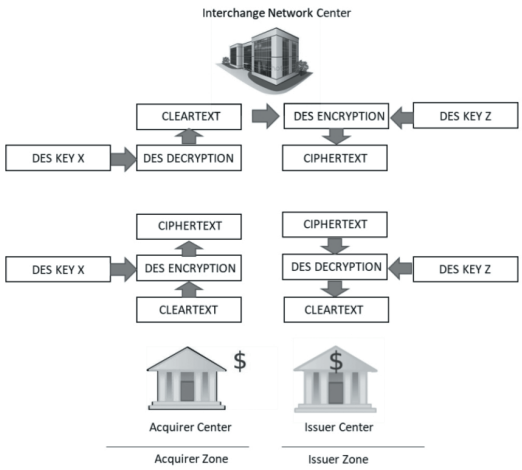

Fig. 1. Interchange Message Path

4. PROPOSED CRYPTANALYSIS

As we noticed in the previous text, the actual algorithm, which is generally used in the protection of payment card data, is DES algorithm. DES algorithm belongs to the group of symmetric algorithms. In addition, DES algorithm is a block cipher system, which means that the data is dividing into the blocks size of 64 bits or 8 bytes. Having on mind the fact that the enciphered PIN value, PVV is just 4 digits long, there is a possibility to recalculate clear text PIN value. What we suggest is using brute force attack or exhaustive key search to PVV in order to recalculate original PIN.

The issuers usually creates PIN value that consists of 4 digits although the number of digits can be up to 12 digits, as it is described in the previous text. The main reason for such length is facilitating the humans to remember the PIN. The number of possible combination for PIN value is 10.000, from 0000 to 9999. Trying all possible combinations on the ATM or POS, most likely will be unsuccessful. As it is mentioned in the previous text, the number of attempts to enter PIN value is limited. The number of attempts depends on the issuer, but commonly used number of allowed attempts is 3 after which the card is blocked. So recovering PIN on the ATM or POS is not an option.

We suggest copying PVV value to the local computer and doing the cryptanalysis on local equipment in such a way that the payment system has no information about the attack. The number of attempts in such a scenario is unlimited. When the PIN is revealed, the card can be used on ATM or POS without any obstacles. In that way attacker can bypass the Card Operating System - COS on the chip and the whole system of the cryptographic

keys which is partially described in the previous text. The brute force attack can be performed by specialized software or hardware.

A brute force attack on DES requires a single plaintext/ciphertext pair. Another plaintext/ciphertext pair is useful to confirm the result once found and rule out a false positive. It can be concluded that if attacker knew one PIN/PVV pair for a particular bank and a particular type of card, the attacker did a brute force attack and revealed the DES key. The same algorithm and the same key are valid for the other cards of the same bank and the same type of card.

If the attacker legally owns a bank card he knows the PIN and PVV at the same time which means that he knows the clear text and enciphered text. At the same time, the attacker knows the applied algorithm. If attacker is performing attack on local resources, it will not violate limitation number of PIN attempt input.

Capacities of the hardware and processors power might be an issue, but if the attacker performs using the capacities of other computers thus doing the parallel processing, the problem can be resolved relatively quickly.

In order to speed up the process from mathematical perspective it is good to have on mind the following:

DES key search with a single PIN/PVV using a black-box DES implementation requires 2^{56} invocations in the worst case. Discounting the "optimization" of concluding after 2^{56}-1 keys did not match that the single remaining one must be right, which is unrealistic, and saves only 2^{-56} of the effort with odds 2^{-56}. There will be 2^{55} invocations on average, the expected time/effort. Chance/risk, depending on point of view by attacker/user, that the key is found after only 2^t tests is 2^{t-56} for $t \leq 56$ using sequential key search, or $t<<56$ using random key search [15].

5. CONCLUSION

In this text we described some basic elements and methods of payment cards and analyzed their interdependencies. The weakness of PIN protecting presented in this paper points to the vulnerability of whole bank card system regarding the bank cards with magnetic stripe and bank cards with chip. It is shown that there is a significant probability to reveal the PIN value and unauthorized use of counterfeited card on the ATM and POS as well. The observed vulnerability can be exploited widely even from the attackers who are neither top skilled in cryptography nor in programming. The danger for the bank card system is huge. As it was previously said, over 90% of world's money is digitalized so the danger is almost unimaginable.

If banks take our work into consideration they will conclude that it is necessary to change the PIN protection, which has been in use for over a four decades. It is ultimate time for applying the new system of PIN protection while it is not too late. We tried to make an alert and we hope that this article will initiate changes that will secure the digitalized currencies. Capacities of the hardware and processors power might be an issue, but if the attacker performs using the capacities of other computers thus doing the parallel processing, the problem can be resolved relatively quickly.

REFERENCES

[1] Deutsche Bundesbank Jahresbericht, Frankfurt am Main, Deuchland, 2016.

[2] Goran Kunjadić, Zoran Jović, Bitcoin - Banking and Technological Challenges, FINIZ 2016 - Risks in Contemporary Business, 2016, DOI: 10.15308/finiz-2016-185-189.

[3] Banking - Secure Cryptographic devices (Retail) ISO 13491.

[4] Personal Identification Number Management and Security, ISO 9564.

[5] Personal Identification Number (PIN) Management and security ANSI X9.8.

[6] Payment Card Industry Data Security Standards – PCI DSS Standards.

[7] Mladen Veinović, Saša Adamović, Kriptologija I, Univerzitet Singidunum, Beograd, Srbija, 2013, ISBN: 978-86-7912-469-2.

[8] Milan Milosavljević, Saša Adamović, Kriptologija 2, Univerzitet Singidunum, Beograd, Srbija, 2017, ISBN: 978-86-7912-653-5.

[9] Data Encryption Algortihm, ANSI X3.92.

[10] Banking Key Management (Retail) ISO 11568.

[11] Retails Financial Services Symmetric Key Management Part 1: Using Symmetric keys ANSI X9.24.

[12] Financial Transaction Card Originated Messages ISO 8583.

[13] Modes of Data Encryption Algorithm Operation ANSI X3.106.

[14] Triple Data Encryption Algorithm (TDEA) Modes of Operation ANSI X 9.52.

[15] Tingyuan Nie, Teng Zhang, A study of DES and Blowfish encryption algorithm, TENCON 2009 - 2009 IEEE Region 10 Conference, IEEE, DOI: 10.1109/TENCON.2009.5396115.