

PIN Debit Payment with PC Software? No, Thanks!

Jimmy Tang, Ken Mages - HomeATM

The PIN Debit Payment Experience

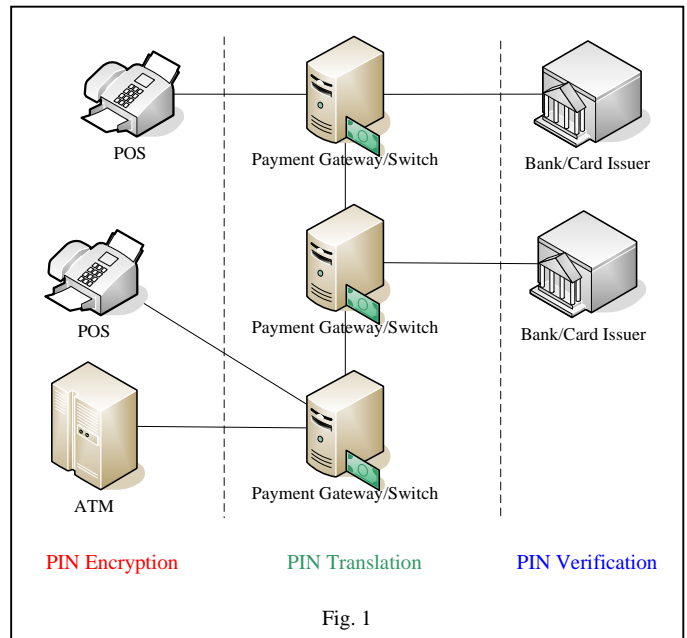
Let's review the PIN Debit payment process in the brick and mortar world and see what is going on behind the scenes:

1. A customer uses his/her debit card to pay for something at a checkout counter with a POS (Point of Sales) terminal or withdraw cash at an ATM (Automatic Teller Machine).
2. He/She swipes his/her debit card across a magnetic stripe card reader on the POS terminal. The terminal reads the track data known as Track 2 encoded on the card [7]. Track 2 contains information such as PAN, the Primary Account Number of the debit card.
3. He then enters his PIN (Personal Identification Number) into a PIN entry device (PED) [1]. Inside the PIN entry device, an EPB (Encrypted PIN Block) is formed. The PIN in clear-text only exists ephemerally inside the PIN entry device. The output from the PED is in an encrypted format.
4. The resulting EPB and Track2 are packed with other transaction data such as amount, transaction number, etc. into a transaction message in a specific format (e.g. ISO-8583). Since there are usually no direct connections between the POS and the Issuer, the message has to be forwarded to payment switches for processing. In each payment switch along the chain of processing, the incoming EPB is decrypted with a key associated with incoming EPBs. After decryption, the plaintext Pin Block is reformatted if necessary and encrypted under another key to form the outgoing EPB. The EPB is thus translated, referring to the change of the encryption key and also the possible reformatting to a different PIN Block format.
5. After traversing all the switches, the transaction message arrives at issuer where the PIN is verified. Given that the account has sufficient funds, if the PIN passes the verification, money is debited and the transaction succeeds. The response from the issuer is then transported back along the original path to the POS/ATM terminal.

In the process above, we see three types of PIN operation:

1. PIN Encryption at the PIN Entry Device
2. PIN Transaction at the Switch
3. PIN Verification at the Issuer

These PIN operations, along with PAN capture, will be further discussed in the following sections.



Card Swiping and PIN Entry

We should all be very familiar with the swiping a card or keying in a PIN at the ATM or POS terminal. The ease and security are taken for granted. In fact, there is a set of strict rules to regulate the handling of PIN and sensitive data. Each POS/ATM encrypts the PIN entered so that the plain text PIN is NEVER exposed outside that device [1].

When PIN debit comes to the internet, the nature question to ask is obviously: Can we use the PC alone as a PED? The simple answer is **No**.

At an online shop, a user operation is done in a browser using input peripherals such as the keyboard or the mouse. Now, how is the card data or the PIN captured? If these sensitive data are typed in or clicked in, it is definitely possible that the secure data is captured by some other malicious program running on your machine. Malware such as keyloggers and screen scrapers are not sophisticated and have been lurking around for years.

The next question is how the PIN is encrypted into a EPB using one of the approved PIN encryption algorithms as stated in the literature [4, 5, 6]? This leads to the question of where to store the key and how to do the key management. Then, where is the computation done actually? If the encryption is done inside the computer

processor, it is possible that some malware is able to read the intermediate values. How about the memory leakage of the OS, when intermediate values appear in the memory and remain there? Forming the EPB on the PC is not a wise thing to do, to say the least.

The security level simply cannot be guaranteed without the help of external hardware.

Some people are reluctant to do a payment transaction online, quite independent of the level of their computer literacy. Why? Because the PC is inherently vulnerable.

The problem is greatly amplified by the multitude of possible configurations of browser, operating system and hardware platforms. The surface area of attack is so large that it is virtually impossible to contain the problem at this moment. The attacks can be on the payment software, the browser, the operating system, and even the PC hardware itself. If the PIN exists in any transformed form somewhere, sometime within the PC, it is NOT safe. Typing or clicking a PIN into a browser simply does not work.

Now, the card swipe. The card number is clearly embossed on the card. Can we just type in the number instead swiping? Encoded on the back of the card is a string of electromagnetic patterns that contains the card number as well as other information. Without this data, PIN verification simply cannot be done. (More on this in the PIN Verification section). By swiping a card, it also proves the presence of a card. Card-Present (CP) Transaction enjoys a lower transaction rate because it is more secure. Again, we come to the conclusion that a piece of external hardware is necessary to capture both the PIN and the card data.

PIN Translation

At the switches along the payment path, the PIN blocks are decrypted, reformatted and re-encrypted. The PIN block is said to be translated. The translation itself is a highly sensitive operation and must be done in Tamper Resistant Security Module (TRSM) or Hardware Security Module (HSM) [2]. These hardware modules provide a secure, trusted environment to perform sensitive operations. Note that PIN block decryption is NEVER done

A computer server is no TRSM or HSM.

As mentioned in the previous section, it is not a wise thing to form the EPB inside the PC. If the PIN is encoded/transformed/scrambled or otherwise disguised in some manner in the PC, it means the PIN needs to be recovered at the server in order to pack it with the PAN to form a Pin Block. It follows that the clear PIN text must at some stage appear on the server, which is not something a card issuer expects to happen.

In this scenario, there is PIN decryption and it is not done within an HSM. This transportation and handling of the PIN is clearly NOT one of the approved methods in PIN

management standards [4, 5, and 6].

PIN Verification

The PIN is verified at the issuing bank and the operation occurs only within HSMs.

There are two major algorithms in PIN Verification based on DES encryption algorithms: the IBM 3624 offset (PIN Offset) and the VISA PVV (PIN Verification Value). Both involve a piece of a validation data, a PIN Verification Key (PVK) and a piece of verification data. The piece of verification data is stored on the card or on a database or both.

IBM 3624 PIN Verification

The idea is that a natural PIN is calculated by encrypting the PAN using the PVK. Then the difference, called the PIN Offset, between the customer's selected PIN and the natural PIN is stored on the card. The PIN can be changed if this offset is stored on a database.

VISA PIN Verification Value

In this method, the PAN and PIN is encrypted by a PVK specified by a PIN Verification Key Indicator (PVKI). The result is called the PVV and is stored on the card or a database.

In both cases, some data contained in the magnetic track are used for PIN Verification. The same data can come from a database. But besides PIN Verification, the bank most likely validates other card data such as expiry date and a service code. This depends on the implementation of the issuer. But from operational experience, Track 2 data IS required to perform a debit transaction.

Summary

Secure PIN debit transaction using a PC is shown to be insecure and unfeasible without the help of additional external hardware.

Reference

- [1] PCI Security Standards Council – PIN Entry Devices. https://www.pcisecuritystandards.org/security_standards/pe_d/index.shtml
- [2] FIPS PUB 140-2 Security Requirements for Cryptographic modules
- [3] ISO-8583 Financial Transaction Card Originated Messages – Interchange Message Specifications.
- [4] X9.8 PIN protection principles and techniques for online PIN verification in ATM & POS systems
- [5] ISO 9564-1 Part 1- Basic principles and requirements for online PIN handling in ATM and POS systems
- [6] ISO 9564-2 Part 2 - Approved algorithm(s) for PIN decipherment
- [7] ISO/IEC 7813, Identification cards — Financial transaction cards