

**POINT OF SALES WITH 2-FACTOR AUTHENTICATION**

Manzoor AHMED

Gaurav GUPTA

CS 265 Biometric Project

October 15, 2016

**SECURING POINT OF SALE SYSTEM**

In order to prevent fraud banks are issuing credit cards / debit cards embedded with a small chip called EuroPay MasterCard and Visa (EMV) to their users. Though, criminals have found ways around EMV chips, and they can still steal card data, defeating EMV security. The sole purpose of EMV is to prevent cards from being duplicated, rather authenticating original cardholder.

Nevertheless, adding another security measure, such as biometrics to cards, along with pin number and EVM will make it much more secure for authenticating the original card holder. Provided that for authentication, a user must provide three type of information: ‘Who you are’, ‘What you know’, and ‘What you have’.

Clearly, during authentication, credit card processing companies / banks don’t know if a user has a stolen card, that is the bank does not know for certainty the ‘*Who you are*’ part, thus allowing criminals to impersonate. To solve this problem, banks must use two-factor authentication. Henceforth with two-factor authentication, it will not only make bank profits, but also prevent criminals from impersonating.

Below is a simple infrastructure for solving the above credit card /debit card security problems with simple fingerprints biometrics.

**INFRASTRUCTURE**

The Point Of Sales (POS) systems already has an established infrastructure, just by adding a fingerprint scanner, an LCD screen, antivirus software on the card reader, and antivirus software on the POS system enables existing infrastructure for biometric compatibility on the user side.

Similarly, storing fingerprints data on the bank side is solely adding extra table(s) to existing database. In the same fashion, collecting fingerprints from account holders is just incorporating an optical scanner to an existing bank-end infrastructure, thus enabling existing bank-end infrastructure for biometric.

As an illustration, below is a simple biomimetic infrastructure for POS with a fingerprint, EMV, and pin number authentication.

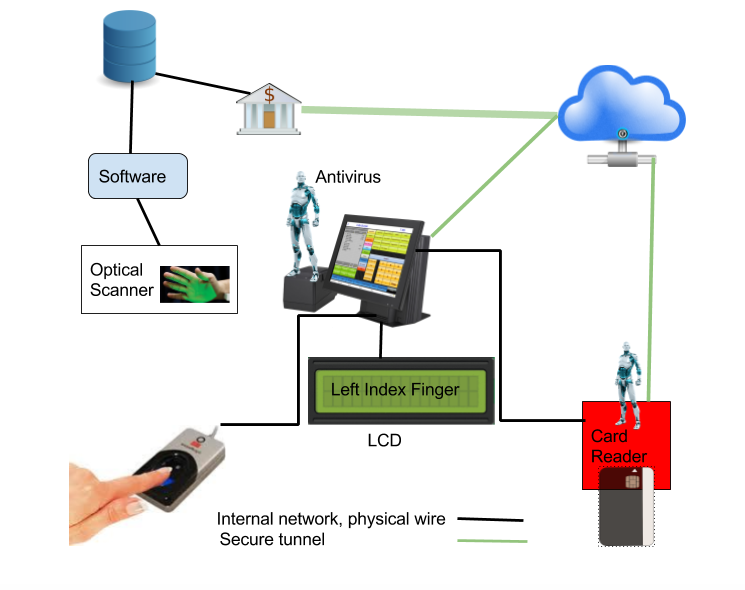


Figure 1: Components of 2-factor authentication

**ENROLMENT PHASE**

In this phase, a bank can either register a new account holder along with his or her fingerprints, or update existing account by forcing account holders to provide fingerprints at its facility. At the facility, each user’s hand(s) are carefully scanned using an optical scanner. Then special software is used, which only extracts fingerprint data from the scanned hand, and decides how to represent each fingerprint as a unique binary code. For example, if a user’s both hands are scanned (assuming the user has two hands and ten fingers) then the software will extract fingerprints from both hands, all ten fingers, and then convert each fingerprint data to a unique code. After, obtaining a unique code from the software, the system admin decides how to link user’s biometrics data with user’s account number.

Below screenshot shows how fingerprints are collected.

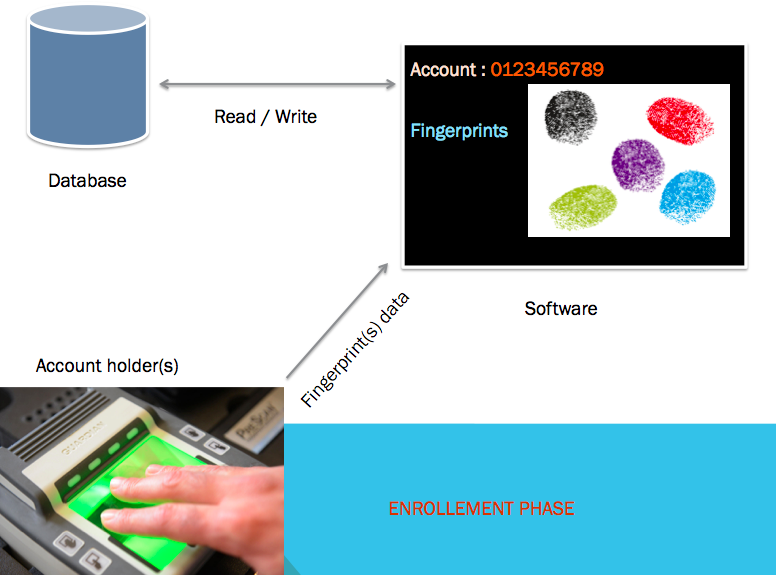


Figure 2: Collecting user’s fingerprints data

In the above figure, once user’s fingers are scanned, software extracts fingerprint scans and converts them to unique code, then stores them in a database. The software can also read fingerprints from the database and represent them on a monitor for system admin, or anyone who is operating the optical scanner, to make sure all fingerprints are being scanned correctly.

Additional users can also be added to a same account by just providing the bank with his/her fingerprints.

After scanning user’s fingers, a system admin would link user’s fingerprints with account number and card number. The below tables represent a very basic approach of storing fingerprints information.

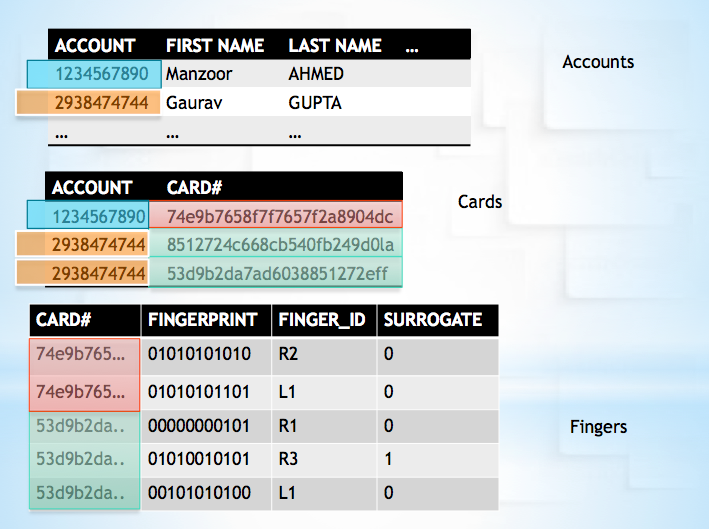


Figure 3: Storing fingerprints and linking with account

For example, **Account** table represents an account holder’s information and one-to-many relationship with **Card** table, and the **Card** table contains all users’ card information, which has one-to-many relation with **Fingers** table. For each unique **Card#**, there are many fingers registered.

In the **Fingers** table column **FINGERPRINT** represents fingerprint code, and the **FINGER\_ID** indicates user's finger information, for example, R2 (Right index finger) and the **SURROGATE** column represents additional users’ finger information. For example, 0 express (original account holder fingerprint), and 1 represents surrogate’s fingerprint.

**RECOGNITION PHASE**

First the user enters his/her card to a card reader, provides the pin number for the card. If the card reader can verify pin number through bank, then the pin number gets sent to the bank along with card information. If not, then the card reader verifies the pin number from user’s card. To prevent card reader from RAM scrapers, there must be an updated RAM scraper blocker installed.

After card user’s pin number validation, the bank check if given card has fingerprints data. The bank decides which fingerprint data should be checked for authentication. For example, if user has 10 fingers registered, then the bank randomly picks one finger out of 10 and sends the requested data to the POS system. An LCD attached to POS system prompts the user, or shows an animation to the user to provide scan for a finger. Card user provides fingerprints by placing finger on the fingerprint scanner, and the POS submits fingerprint data to the bank through a secure channel.

Assume, a bank requires 70% match for authentication, then using different scanners could result in different False Acceptance Rate (FAR); for example, if a vendor is using cheap scanner than it would take many tries to authenticate, but if a vendor uses quality scanner than the user can get authenticate whit less tries.

**SUPPERIROTY & INFERIORITY**

Combining fingerprint scanner with POS makes it significantly secure over the existing infrastructures. As we mentioned earlier in the recognition phase, the bank requires a random fingerprint scan for every transaction to make sure at the time of purchase user can provide a real fingerprint data –*not* forged fingerprint data. For example, assume Trudy has someone's stolen card, and she knows its pin number. In order to make a successful transaction, she must have all ten fingerprints data with her. Even if she has all fingerprints data with her, she would still not be able to make a successful transaction because the bank only gives her certain tries to provide correct fingerprint data before locking the card.

The figure below shows how this attack is possible:

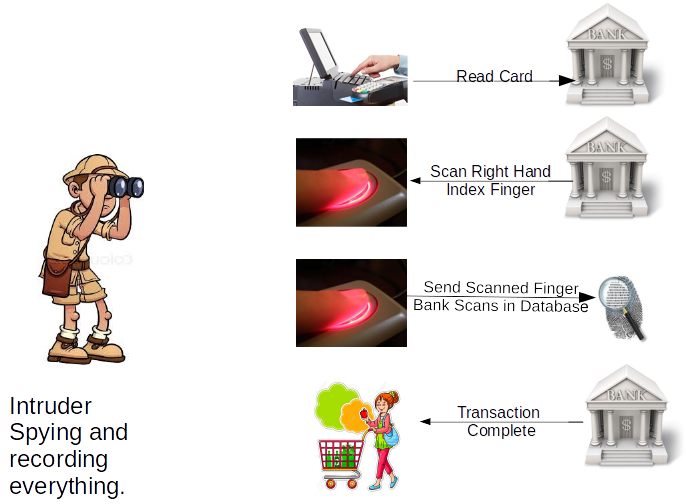


Figure 4: Intruder stealing fingerprints

After monitoring POS systems for prolonged period, eventually an attacker could be successful by collecting all fingerprint data of regular shoppers, shown in the above image.



Likewise, a transaction will fail even when an intruder shown in figure 5 has all card data stolen from the POS or from the card terminal, because when the intruder tries to repeat the steps shown in figure 5, the bank will make the authentication process troublesome for the intruder. To emphasize, it is the bank that makes the request for a fingerprint data, based on the data available within its database. Indeed, any other fingerprint scanned apart from the requested one, would fail the transaction.

Authenticating user with fingerprints adds additional security shield to user's card by authenticating its owners only. Without user's fingerprint the card is in no use, even if it gets stolen or its data gets exposed through RAM scrappers.

**INFERIORITY**

However, there is a very slim inferiority by adding fingerprint scanners to an existing infrastructure because it makes the authentication process much slow, because a user might have to provide fingerprint scan multiple times to get authenticated. Since different types of scanners will be used by different POSs, quality of fingerprints data could differ, resulting in different insult and fraud rate.

Another, drawback with this approach is that in any case if a user's fingerprint data is compromised through other sources, then updating fingerprint will not help banks, unless banks reissue cards to all its users. Additionally, security of POS is distinct; this enables it for either internal attacks or external attacks. To such degree, a frequent user's fingerprint data could be compromised through POS system.

**HARDWARE & SOFTWARE REQUIRMENTS**

As we mentioned, most of hardware and software already exists already in the infrastructure. Just by adding a fingerprint scanner on the user side, and a secure POS and a secure card reader will complete the requirements for 2-factor authentication, using fingerprint biometrics. In the below table, column EXISTS ALREADY marked ‘NO’ gets added to the current infrastructure, also indicating its prince in the PRICE column. Correspondingly, the SIDE column shows where the ITEM is coupled.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ITEM | **CATEGORY** | **EXISTS ALREADY** | **PRICE** | **SIDE** |
| **POS** | SOFTWARE | YES | $ 1500.00 | USER |
| **POS SOFRWARE** | SOFTWARE | YES | $ 40 | USER |
| **POS ANTI VIRUS** | SOFTWARE | NO | $ 40 | USER |
| **CARD READER** | HARDWARE | YES | $ 80 | USER |
| **LCD** | HARDWARE | NO | $ 10 | USER |
| **FINGER SCANNER** | HARDWARE | NO | $ 30 | USER |
| **OPTICAL SCANNER** | HARDWARE | NO | $ 500 | BANK |
| **SCAN CONVERTER** | SOFTWARE | NO | $ 100 | BANK |

Initial setup cost for a new vendor would cost approximately $1930 plus a monthly charge of $80 for software / anti-virus upgrades.

An existing vendor would just require POS software, capable of reading data from fingerprint scanner, attach an extra LCD to the POS, and connect a finger scanner to an existing POS. As mentioned above, adding new biometrics would only cost $250 to the vendor and an additional monthly payment of $40 for maintenance.

Though the bank will have to pay more for this new biometric feature; adding an optical scanner, and adding special software to convert fingerprint data cost the bank almost $600, adding an additional cost of $1 per one million fingerprints data storage.

**Suggested biometric satisfies criteria for "ideal biometric"?**

The ideal biometric should persist the properties of universal, distinguishing, permanent, collectible and reliable robust and user friendly. With the current implementation, it will have all the properties as this could be applied to every individual who possess a credit card from the bank. It is well known fact that the fingerprint differs from one person to another and would not change over a long span of time, at least not before the credit card expires. Collecting fingerprint is also an easy task, which could be done by any individual with the little knowledge regarding the software, since the method is clearly distinguishable and easy to obtain it is clearly user friendly.

As mentioned earlier, we add an additional layer of security over existing infrastructure by taking the credit card holder's fingerprint. This additional layer of security curbs the false acceptance rate by significant factor. The existing infrastructure is based on two type of authentication, "*what you have*" and "*what you know*". Additional security layer implement the third type of authentication "*who you are*". The combination of the three would result into a better infrastructure with less number of frauds.