Biometric Credit Card Verifier

Brittany Hall

Maya Lilley

Advisor: Dr. Farzad Moazzami

December 3, 2015

Abstract:

In this project we will explore the current biometric applications that are used today that help with the advancement of financial technology. We will look at the number of problems within these applications and a way we can make it better. We will then develop a prototype of the final device. This device will generally identify the user by scanning the fingerprint and then prompting the user to swipe their credit card. Each of the inputs from the fingerprint as well as the credit card should both match the information stored in the database; this essentially will reveal if the user is authorized to use that specific card. This method will prevent credit card fraud and will provide a safer way to use your credit card.

Introduction:

In today's society technology is an ever evolving concept that reveals more about itself once a new Theory is learned; there is always a deeper foundation where the concepts, theories, and ideas come from. As technology continues to evolve and grow, there are always users that try to misuse the technology that is available to us; in this case we will discover the idea of Credit Card fraud. A number of individuals have encountered this violating concept of credit card fraud and everyday technology professionals try and figure out different ways this can be totally eliminated. Hackers have become more advanced to the idea of individuals using electronic devices to purchase items. The idea of purchasing items online, using PayPal, credit cards, Apple Pay, etc. is no longer a foreign concept; and unless these items are strongly secured it is very easy for a hacker to access money from whoever they want. In this project we will explore a low level, secured device that will possibly prevent the idea of credit card fraud.

Many people have experienced purchasing items at their local store, using a credit card to purchase their items, and the cashier never asking for any form of idea. Many people have also experienced, the keypad not requiring an actual signature to verify that the card is in the possession of the correct person. This proves that there are gaps within the system that is current and it is important that a new method of verifying credit cards is made. 15 million United States residents have their identities stolen every year

with financial losses of $50 billion, and 29% of those residents indicate that their identity has been stolen from a lost or stolen wallet. When misusers have physical access to a credit card, it is very dangerous in regards to not only the safety and security of your money but also your identity. This small application will prevent the possibility of easy identity theft.

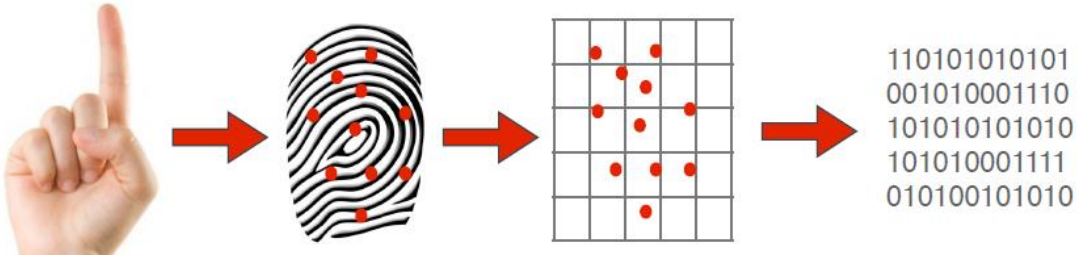
Theory:

There are a number of popular biometric applications used today that try and eliminate the idea of credit card fraud and identity theft; such as Apple Pay, Samsung Pay, and Android Pay. There are also a few applications, that are not operated by biometrics that try to eliminate credit card fraud and identity theft; such as PayPal and the EMV Chip that are now embedded on credit and debit cards. But each of these applications has had their problems.

When setting up an Apple Pay account, it is not verified if the information that is being activated is accurate or not. Someone using the Apple Pay method could enter stolen credit card information and there is no way the local bank would be able to verify. In this case, information that is used could always be inaccurate and it could take months to find out and by then, a massive amount of money is already withdrawn from the account. PayPal is another application that allows users to purchase items online without directly inputting a credit card number; but once again the problem with this application is, inaccurate information can be inputted and by default money is withdrawn from the PayPal account without the user knowing. The EMV (Europay, Mastercard, and Visa) Chip is another current system that tries to make the transaction experience more secure. But this chip has statistically proven to add an additional 20 seconds to the average checkout time, and if the chip is embedded on a debit card, the checkout terminal forces the user to use credit. These are flaws within these applications that hinder users from a smooth and safe transaction experience.

This project will introduce a simple way to verify the user that has possession of the card. We will use biometric technology in order to confirm the accuracy of the verification.

Biometrics is automated methods of recognizing a person based on a physiological or behavioral characteristic. A fingerprint scanner system has two jobs -- it needs to get an image of your finger, and it needs to verify the finger scanned matches with previous scans of this finger. Only specific characteristics, which are unique to every fingerprint, are filtered and saved as an encrypted biometric key code. Captured images are not saved only the series of numbers in binary code is used for verification, unless authorized by a system. Algorithms obtained from a fingerprint cannot be converted to an image, which emphasizes that no one can duplicate your fingerprint. Fingerprints are much harder to fake than identity cards as well. You cannot guess a fingerprint pattern like you can guess a password, you cannot misplace your fingerprint, like you can misplace an access card, and you cannot forget fingerprints like you can a password.



Digital Persona 4500 Fingerprint Scan: Finger print reader that comes with a specific API, this SDK is able to capture images, fully embraces image, template and compression standards. Provides flexibility within the software to match algorithms and save data. This device is compatible with Windows XP, 7, and 8.1. In order for the device to work you must have a U.are.U SDK for Windows. The SDK is also known as a Software Development Kit; they are tools that allows the creation of applications, a library that facilitates usages of an API (Application Programming Interface).

.

Credit Card Swipe :

Credit card readers (also known as MSR or magistrate readers) are an essential part of any POS system. Credit card readers are designed to read the information encoded in the magnetic stripe located on the back of a card or badge.

Compatible: With any computer. No specific software needed. Write the numbers seen on a card in any application.

Materials

Digital Persona 4500 Fingerprint Scan

Credit Card swipe

Laptop

Windows XP

Microsoft Visual Studios

Digital Persona SDK

Project budget:

Digital Persona Software Development Kit	$150.00
Digital Persona Fingerprint Scanner	$73.00
USB Credit Card Reader	$16.99
Windows XP	$39.99
ThinkPad Laptop	$399.00
Visual Studios 2010 (Downloadable)	Free

Procedures:

1. Obtain all necessary materials. (Digital Persona 4500 Fingerprint Scanner, Credit Card swipe, Laptop with Windows XP/7/8.1, Microsoft Visual Studios, and Digital Persona Software Development Kit).
2. Install Microsoft Visual Studios and the Digital Persona software development kit onto the laptop.
3. Once the software is installed, open the software development until the file for the sample codes are opened. Choose the language of preference, (i.e. C++, C#, Java).
4. Once the sample code is opened, connect the digital persona 4500 fingerprint scanner to the laptop.
5. In order to test that the device is working properly, open the software development kit sample code, compile the program, click capture.
6. Once capture window pops up, place any finger on the fingerprint scanner. Hold finger on scanner until the device captures and image that you can see on your laptop.
7. If the device is working properly, familiarize yourself with the sample code and thoroughly understand the language.
8. Once the software development kit is opened and the GUI is shown on the laptop screen, click on each of the options (i.e. Verification, Capture, and Enrollment) and place finger on the device once the option is selected. This will provide you with an understanding of how the software development kit works. Please keep in mind that this kit is not designed to do everything you may want it to do; these steps are strictly to familiarize yourself with the device and how it works.
9. Once you are familiar with the software development kit, connect credit card swipe to laptop via USB (If the fingerprint scanner is already connected and you only have one

USB port, remove the fingerprint scanner and connect the credit card swipe. If you have multiple USB ports on you laptop, use another port for the credit card swipe).

10. Open up another project in visual studios, and swipe a card with a magnetic strip and observe what pops up. (This device can also work with Microsoft word, Matlab, or Notepad)
11. If the credit card swipe outputs information accurate to the card that was just swiped, the device is working properly.
12. Since there is no software or software development kit for the credit card swipe you will have to build an original code that will recognize the person whose card is being swiped. (i.e. If John Doe has card number 4637382872, the code should identify that when the card 4637382872 is swiped the program should state, “Hello John Doe”)
13. Once the code for the credit card swipe is complete and the software development kit for the fingerprint scanner has been observed, the two devices can now be put together. The only part of the code that will need to be manipulated is the verification section of the code.
14. When looking at the verification code for the software development kit you must observe the area where the code is matching the first fingerprint. Note: This is where you will begin to integrate the credit card code you created in step 12 and the fingerprint scanner verification code.
15. Take the section from the credit card swipe code that stores the credit cards into the database and place that section into the verification code, right before the fingerprint matches the next fingerprint input. Note: Make sure that the syntax of the codes includes all of the libraries they are supposed to have.

16. In order to match the input of the fingerprint with a fingerprint in stored, you must save the fingerprint binary numbers to a database. And in order to save the binary numbers to a database you must look at the capture code and instead of outputting an image, you must change that to binary numbers. Note: Change the image prints out to a binary print out, this will provide you with the binary features of the fingerprint image and not the image itself. This will allow you to store the features into a database.
17. Once each database has accurate information stored in both of them you should be able to test out each of them separately.
18. In order for the codes to work together they must be connected through a file. The fingerprint scanner must read the file and then a function should allow the credit card code to automatically compile. This will allow the two codes to work together and it will make the process user friendly.

Results:

As a result of this Biometric Credit Card Verifier, we were able to successfully create a prototype of a credit card terminal that has a fingerprint scanner attached to it for verification purposes. This will prevent the number of identity thefts that happen within a years' time frame. By manipulating the verification code that was given within the Digital persona SDK, it allowed us to get the fingerprint scanner to do what we essentially wanted it to do. Once we integrated both of the codes, we created a prototype that successfully printing out three different statements. If you had a fingerprint that was stored in the database and a credit card that was stored in the database, the message would say, "Hello 'user'. Access Granted" If you have a fingerprint that is in the database but the wrong credit card, the message will say, "Transaction Denied. Please try a

different card.” And if you scan a fingerprint that is not stored in the database then it will not allow you to make it to the next phase of the transaction, which is swiping your card. The prototype proves that we have successfully created a Biometric Credit card verifier.

Conclusion:

As technology continues to advance, we experience a number of risks that leave us vulnerable to applications that we use. We have used a number of biometric applications that have been created to prevent and eliminate credit card fraud and identity theft. Many people use Apple Pay, Samsung Pay, and Android Pay. These are biometric applications that are commonly used. There are applications that are used that are not centered on biometrics, such as PayPal and the EMV chip that is embedded in your credit card. Each of these applications has problems that hinder the purpose of these applications. We have created a new application that allows users to verify their credit cards before every transaction. In theory the user scans their fingerprint, if their fingerprint is in the database, the system prompts the user to swipe their credit card. In order for the transaction to go through the user must have a registered fingerprint and credit card; meaning both have to be in their separate databases.

In order to create this prototype there are a number of items that need to be obtained. You must have a fingerprint scanner, a credit card swipe, a SDK (Software Development Kit), Visual studios, and a laptop. Once each code is written, for the credit card as well as the fingerprint scanner, you can now integrate each code together.

The goal of this application was to create a biometric verifier and we successfully accomplished that.