Credit Card with Biometric and Other Securities (C C BOSS)

Mohammad Sajid Qamruddin Khizrai¹,

¹PG Scholar Priyadarshini Institute of Engineering & Technology, Nagpur
Sajid4u0023@gmail.com

ABSTRACT
Credit card is a very important card, it is treated as cash in a pocket or (vollet) a person took few hundred’s or thousand in his pocket, if a pocket is lost, a person lost few hundred’s or thousand. But the loss of credit card is very big loss (few lacs ) depending upon the credit limit. A person who got this card can purchase up to the limit of credit card from single shop or with different shop. And a shopkeeper never asks the ID’s of card holder and not match the ID’s with credit card’s name.

In our PROPOSED (C C BOSS) features in security, if person loss his credit card then will not worry about any loss of money using this credit card.

Keywords: Credit Card, Biometrics Security

1. INTRODUCTION

Different security industry for Credit cards, Debit Cards and online transaction is using highest level of Personal Identification Number (PIN) security. The confidentiality of cardholder PINs being accepted and processed at Point-of-Sale ("POS") PIN-Entry Devices ("PEDs") and Automated Teller Machines ("ATM") depends on all payment system participants doing their part with implementing and maintaining the applicable Payment Card Industry (PCI) PIN Security Requirements, PCI Point of Interaction (POI) Modular Security Requirements and Visa Requirements [1].

Small businesses such as restaurants that use an older generation of countertop credit card terminals may be breaking the rules inadvertently because the device stores magnetic stripe data or otherwise violates the PCI requirements. So consider upgrading to a payment device that is certified PCI compliant. Basic terminals capable of encrypting Personal Identification Number (PIN) codes and protecting other sensitive information are available. The PCI Security Standards Council publishes a list of approved devices. Just remember that using a compliant device is only one element of making your business compliant.

Even if you’re not storing anything explicitly prohibited, you may be storing more credit card data than you need to. Small merchants typically store a day’s worth of credit card numbers on a card swipe terminal, then process all the transactions in a batch at the end of the day. Bigger retailers may record the card numbers in a centralized database so they can track all a customer’s purchases, and so they can retrieve the number if they need to issue a refund. But do you need to retain those numbers at all?[2]. This information is can be used by other person in online transaction, this fraudulent of online can be stop with the proposed method.

Many companies using the different techniques to save the data which is stored in magnetic tape of the card, when it is swap in a counter i.e. standards cover everything from the point of entry of card data into a system, to how the data is processed, through secure payment applications. We seek to protect and educate industry players such as merchants, processors, financial institutions, and any other organizations that store, process, and transmit cardholder data, around the world.. [3] This type of security can also be cracked by different software, there is no personal security( Question and Ans) from card holder.

Cardholder Data/ Payment Card Data is all personally identifiable data about the cardholder (i.e. account number, expiration date, data provided by the cardholder, other electronic data gathered by the
merchant/agent, etc.). This term also accounts for other personal insights gathered about the cardholder, i.e., addresses, telephone numbers, magnetic stripe data and CVC2/CVV2.[4]

The Payment Card Industry Data Security Standard (PCI DSS) for securing credit card information while using the Cisco® Unified Customer Voice Portal (CVP). Cisco CVP is an interactive voice response (IVR) product with a unique architecture that lends itself to safe, secure deployment for applications taking credit cards for payment or verification. This document describes the architecture for a Cisco Unified CVP deployment that provides a recommended architecture for credit card safety and security. Cisco Unified CVP may be used in self-service applications that involve the verbal or electronic entering of credit card information as part of a credit card approval transaction. The security of this credit information needs to be considered as part of any PCI-compliant implementation. This document looks at Cisco Unified CVP in the context of a secure architecture design for PCI. It discusses how Cisco Unified CVP would be deployed in that model and how its components would map to the components of the PCI standard. Cisco PCI design guides are available at [6].

What is the Payment Card Industry (PCI) Data Security Standard (DSS)?

The Payment Card Industry (PCI) Data Security Standard (DSS) applies to all businesses, large and small, in any industry, that process, transmit, or store credit card transactions and cardholder information. The goal of the PCI DSS is to increase protection of credit card information and related transactions. Any product that processes, stores, or transmits cardholder data falls under PCI DSS and is subject to a PCI audit[5].

In our PROPOSED (CC BOSS) features in security, if person loss his credit card then he will not worry about any loss of money using this credit card. Because here we are giving a very interesting features in CC, we are giving the security in both type of mode of payment.

1) Direct purchase from cash counter.

2) Purchase online.

1) At present credit card’s figure is look like this.

   FRONT site

   Fig (a)

   BACK site

   Fig (b)

   Example of Some other international Credit Cards
Fig (c)

1) **Direct purchase from cash counter.**

**Drawback:**
1) There is no identity of card holder, it’s sufficient that a person having credit card, OR it’s enough.
2) Shopkeeper will took a card and swap it, he do not check the identity of card holder.
3) At present Shopkeeper not worry about that a card could be stolen by pickpocketer OR any other means.

2) **From Purchase online: At present.**

1) If a person having credit card on his hand, he can purchase directly from online easily, every data is present on credit card for online shopping.
2) At present a verification code is send on a mobile for online shopping. What will happened, if a Lady Purse is stolen from her car and having Credit card and Mobile in it. **then?**

In the propose CC BOSS we are giving the securities in both type of transaction mode.

3) **In Direct purchase from cash counter.**

We will provide securities with the following features
1) On the card we provide photo of the card holder in Figure (d).
2) On the card we provide biometric securities of the card holder on magnetic tape. It will also swap in Figure (e).
3) On the card we provide the mobile no of the card holder in Figure (d).

This is needed if the image of the card holder is blurred then the shopkeeper will call the no. printed on cc.
In our proposed CCBOSS Method.

Ans: No

4) Purchase online:
In online transaction system will call directly to the card holder, and ask that “You are shopping online with this bank with this amount”

First system will ask the security QUEST ? before releasing the payment from the account,

1) if he replied “Yes” then system will release the amount.
2) if he replied “NO” then the fund will not release.

And card will be block temporarily automatically.
Flowchart (2)

System call

Ask, You are purchasing online

Yes
Will ask security code & then fund will Release.

No
Fund will not release

Temporarily Block Card.

References


AUTHOR

Mohammad Sajid Qamruddin Khizrai received the B.E (Computer Technology) 2002 and Pursuing M.Tech degrees in Computer Science Engineering from Priyadarshini Institute of Engineering Technology in 2013 and 2014. During 2006, he worked in “Doha Asian Games 2006” as Wi-Fi Technician in Doha Qatar. In 2007-2008 he has also worked as Network Technician in King Saud University in Kingdom of Saudi Arabia.