International Journal of Engineering Research and Development
ISSN: 2278-067X, Volume 1, Issue 9 (June 2012), PP.15-18
www.ijerd.com

The Study of Fraud Analysis & Securing Card Present Transactions

Mohammad Asim[1], Jamal Mohammad Aqib[2], Khaja Moizuddin Mohammed[3]
[123]*Lecturer, Department of CSSE, University of Hail, Kingdom of Saudi Arabia*

Abstract—*Usage of payment cards such as credit cards, debit cards are growing rapidly in the modern age.Cashless payment system gained lot of popularity in the early 20s and more likely to grow in near future. Plastic money has made life much easier for all of us. But unless we have had a personal experience, we don't realize how much of a security nightmare it can be. Here are a few things that will make our card transactions safer. Unlike magnetic stripe cards, chip cards (also called EMV cards) use superior technology that helps guard against skimming and cloning. When we swipe our card at shopping malls and restaurants or use it at the ATM to withdraw cash and pay utility bills, we are under the constant threat of our cards being counterfeited. Besides, if you lose your card, someone can misuse the time lag, between your losing and blocking the card, to swipe and imitate your signature at the point of sale (POS).*

Lack of adequate security and authentication procedures specifically in card present transactions(i,e transactions at POS and ATMs) have led to billions of dollars losses annually.

This paper mainly discusses the relevant study of fraud of card present transactions(i,e transactions at POS,ATMs) in the country. This paper also discusses the current payment infrastructure available in country and future infrastructure developments for better security and customers satisfaction.

Key words—*POS, PIN, EMV cards, Security Nightmare, Plastic Money, Skimming & cloning.*

I. INTRODUCTION

Plastic money has made life much easier for all of us. But unless we have had a personal experience, we don't realize how much of a security nightmare it can be. Here are a few things that will make our card transactions safer. Unlike magnetic stripe cards, chip cards (also called EMV cards) use superior technology that helps guard against skimming and cloning.

When we swipe our card at shopping malls and restaurants or use it at the ATM to withdraw cash and pay utility bills, we are under the constant threat of our cards being counterfeited. Besides, if you lose your card, someone can misuse the time lag, between your losing and blocking the card, to swipe and imitate your signature at the point of sale (POS)[1].

Millions of dollars loss each year because of payment card fraud has exposed the security weaknesses in traditional payment card processing system.[2].

According to the series of biennial survey conducted by American Bank Association (ABA) issued a report says that:

- Industry check-related losses amounted to an estimated $1.024 billion in 2008, up slightly from the $969 million in 2006. The number of fraud cases also increased.
- Industry losses from debit card fraud—POS signature, POS PIN, and ATM transactions combined—reached an estimated $788 million in 2008[3].

Card Present Transactions (transactions at POS and ATMs) constitute the major proportion of card based transactions in the country. Currently, transactions using cards at POS do not require additional authentication in majority of the cards. Further, data stored in magnetic stripe is vulnerable to skimming. Increasing confidence of the customer for using POS channel would require securing of these transactions through implementation of authentication in the short run and prevent counterfeiting of cards by migrating to chip and PIN in the long run.

This paper focusing the issue to examine all aspects related to use of cards at POS and ATMs and recommend action plan for enabling, additional authentication of transaction using existing cards in a cost effective manner.

II. A SURVEY REPORT OF FRAUD ANALYSIS IN INDIA

The survey finds that banks in India lag in security of cards transactions. "Against the backdrop of well known global cases of card breaches, it is surprising to note that basic measures for ensuring card security have not been adopted by many of the banks," points out the survey done by the Data Security Council of India and KPMG, under the aegis of CERT-In (Computer Emergency Response Team), the cyber security wing of the ministry of information technology.

In all, 20 public sector, private and foreign banks were surveyed and their chief information security officers (CISOs) interviewed for the study. The survey found that banks still follow highly risky practices such as storing and printing authorization information like CVV (Card Verification Value) numbers and expiry dates, and non-masking of card numbers. Merchants are allowed to create card records in plain text. All such practices followed by banks are "non-conformant to globally accepted practices for card security," the survey report states [4]

2.1 Point of Sale (POS) - Fraud Levels

In the context of terms of reference, two categories of frauds are relevant: Lost & Stolen card fraud and Counterfeit card fraud. The total industry lost & stolen and counterfeit card fraud is Rs. 13 crores. The fraud to sales ratio is approximately 1.4 basis points (bps). However, a trend in counterfeit card fraud is that counterfeiting typically happens when customers travel Internationally [5].

2.2 ATM - Fraud Levels

Currently, banks separately report credit and debit card frauds. However, channel wise classification is not available [5].

III. CURRENT USAGE & SECURITY PROCEDURES IN CARD PRESENT TRANSACTIONS

3.1 Magnetic Stripe Cards

The stripe on the back of cards is a **magnetic stripe**, often called a **magstripe**. The magstripe is made up of tiny iron based magnetic particles in a plastic-like film. Each particle is really a tiny **bar magnet** about 20-millionths of an inch long.

The magstripe can be "**written**" because the tiny bar magnets can be **magnetized** in either a north or South Pole direction [6]. The magstripe on the back of the card is very similar to a piece of cassette tape. A magstripe reader can understand the information on the **three-track stripe**.

Fig 1: Magnetic Stripe Card

There are three tracks on the magstripe. Each track is about one-tenth of an inch wide. The ISO/IEC standard 7811, which is used by banks, specifies:

- Track one is 210 bits per inch (bpi), and holds 79 6-bit plus parity bit read-only characters.
- Track two is 75 bpi, and holds 40 4-bit plus parity bit characters.
- Track three is 210 bpi, and holds 107 4-bit plus parity bit characters.

Your credit card typically uses only tracks one and two. Track three is a read/write track (which includes an encrypted PIN, country code, currency units and amount authorized), but its usage is not standardized among banks [7].
Because all relevant information is stored at magnetic stripe itself and at this moment there is no method to verify the identity of the owner. Card can be easily compromised once it is being stolen and lost. The usage of the cards at ATMs even though required a PIN that may also be compromised. So, there is a need of better security and technology for securing card present transactions.

IV. PROPOSED SECURITY ENHANCEMENT FOR CARD PRESENT TRANSACTIONS

4.1 Proposed Security Enhancement for ATM & POS

Most of the cards issued by the banks do not required any PIN at POS or any other means to verify the identity of the owner.

The proposed methods define 3-tier architecture for strengthening the current authentication of card present transactions (POS & ATMs) .The scheme defines the following guidelines and procedures shown in the figure 2.

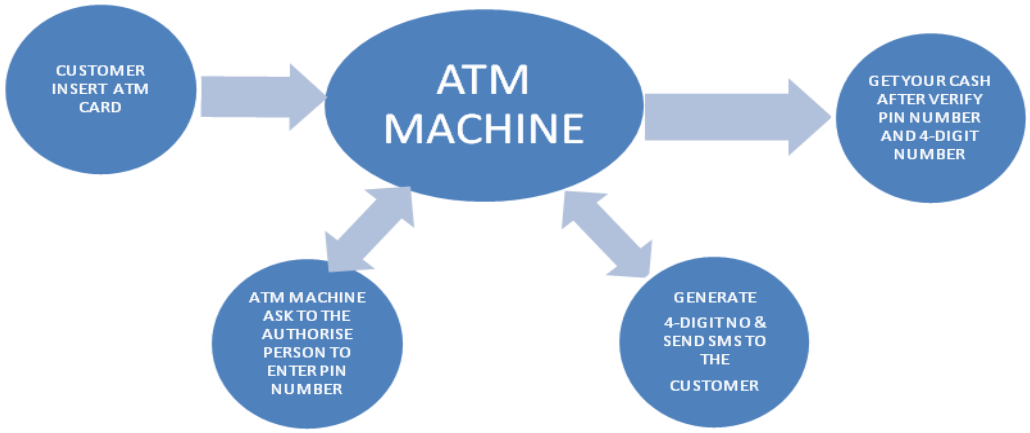

Fig 2: Proposed Process of ATM Architecture

1. Card reader should be capable for accepting PIN for ATMs as well as POS transactions.
2. Third Authentication required a security code through SMS received by the user after successful verification of the PIN on his/her registered mobile number.

Implementing the above methods of authentication require the following modification in the current infrastructure.

1. Terminals will have to be modified to prompt for PIN as well as accepting four digit security code generated by the bank server.
2. If the service code on the card does not support PIN prompt, then terminals will have to be updated BINs (Bank Identification Numbers) of all the issuing banks in India. This has to be done by updating the application software loaded on the POS terminal.

Magnetic Stripe Card and PIN fulfills the short term objective of protecting against lost and stolen card frauds.

V. PROPOSED EMV CHIP CARD

5.1 What is EMV(**E**uro **M**aster **V**isa) **card ?**

Unlike magnetic stripe cards, chip cards (also called EMV cards) use superior technology that helps guard against skimming and cloning.

The EMV Integrated Circuit Card Specifications for Payment Systems are global payment industry specifications that describe the requirements for interoperability between chip based consumer payment applications and acceptance terminals to enable payment. The specifications are managed by the organization EMVCo. named after the original organizations that created the specification, **E**uropay, **M**asterCard and **V**isa.

Fig 3: EMV Chip Card

The distinguishing feature of EMV is that the consumer payment application is resident in a secure chip that is embedded in a plastic payment card, often referred to as a chip card or smart card, or in a personal device such as a mobile phone. The chip provides three key elements - **it can store information**; **it can perform processing**; and because it is a secure element, **it is able to store secret information securely**, and perform cryptographic processing. These capabilities provide the means for secure consumer payments.

In order to execute a payment, the chip must connect to a chip reader in an acceptance terminal. There are two possible means by which this physical connection may be made which are often referred to as *contact* or *contactless*. With contact, the chip must come into physical contact with the chip reader for the payment transaction to occur. With contactless, the chip must come within sufficient proximity of the reader, (a maximum of 4cm), for information to flow between the chip and the acceptance terminal. In both scenarios, the acceptance terminal provides power to the chip to enable the chip to process.

Chips that are embedded in form factors such as plastic payment cards may support only a contact interface, only a contactless interface, or both contact and contactless. Chip cards that support both contact and contactless interfaces are referred to as dual interface. When the chip is installed inside a non-card form factor, such as a mobile phone, contactless is typically the only option for connection to the acceptance terminal [8].

5.2 Why EMV?

EMV is designed to significantly improve the security for consumer card payments by providing enabling features for ***reducing*** fraudulent payment that results from ***counterfeit*** and ***lost and stolen*** cards.
The features that are defined by EMV are as follows -:

1. ***Authentication of the chip card*** to verify that the card is genuine so as to protect against counterfeit fraud for both online authorized transactions and offline transactions.
2. ***Risk management parameters*** to define the conditions under which the issuer will permit the chip card to be used and force transactions online for authorization under certain conditions such as offline limits being exceeded.
3. Digitally signing payment data for ***transaction integrity***.
4. More robust ***cardholder verification*** to protect against lost and stolen card fraud for EMV transactions.

Counterfeit and lost and stolen card fraud represents significant cost to all participants in the payment process, including retailers, acquiring banks, card issuers and cardholders. Costs are realized through the processing of cardholder disputes, research into suspect transactions, replacement of cards that have been counterfeited or reported as lost and stolen, and eventual liability for the fraudulent payment itself. By reducing counterfeit and lost and stolen card fraud, EMV offers real benefits to retailers, acquirers, card issuers and cardholders [8].

VI. CONCLUSION

Study revealed that the customers are on high risk of using magnetic stripe cards which has no or minimum security in the current scenario. We have presented a scheme for the magnetic stripe cards adopting some extra features and keeping minimum changes in the current configuration. Paper also proposed another alternate (EMV chip cards) to improve security to reduce fraud, skimming & cloning. Banking industry required to invest huge amount to replace the existing cards which directly put considerable financial burden on the customers.

REFERENCES

[1]. http://www.thehindubusinessline.com/features/investment-world/article2840227.ece
[2]. Proceedings of the 14th International Workshop on Research Issues on Data Engineering:Web Services for E-Commerce and E-Government Applications (RIDE'04).
[3]. http://www.aba.com/Surveys+and+Statistics/2009_Deposit_Fraud.htm
[4]. http://indiatoday.intoday.in/story/indian-banks-not-taking-data-security-very seriously/1/129039.html
[5]. http://www.rbi.org.in/Scripts/BS_ViewPublicationReport.aspx
[6]. http://money.howstuffworks.com/personal-finance/debt-management/magnetic-stripe-credit card.htm
[7]. http://money.howstuffworks.com/personal-finance/debt-management/credit-card2.htm
[8]. http://www.emvco.com/best_practices.aspx?id=217.