Rovaniemen
ammattikorkeakoulu
University of Applied Sciences

ROVANIEMI UNIVERSITY OF APPLIED SCIENCES

SCHOOL OF TECHNOLOGY

Degree Programme

Thesis

CREDIT CARD SECURITY

Anup G.C.

2013

Supervisor: Jouko Teeriaho

Approved _____2013_____

The thesis can be borrowed.

Rovaniemen ammattikorkeakoulu
University of Applied Sciences

CONTENTS

1. INTRODUCTION……1

2. CONCEPTS……3

2.1 HISTORY OF CREDIT CARDS……3

2.2 BANK CARDS……4

2.2.1 Debit and Credit Cards……4

2.2.2 Working Mechanism……5

3. OCCURRENCE OF BANK THEFT……6

3.1 IDENTITY THEFT……6

3.2 STEALING CREDIT CARDS……7

3.3 PHISHING……8

3.4 BREAKING INTO SERVERS……8

3.5 FALSE TRANSACTION BY MERCHANT……9

4. EMV ……10

4.1 WORKING MECHANISM……10

4.1.1 EMV Contact……11

4.1.2 Contactless Payment Cards……11

4.2 BENEFITS OF EMV……*12*

5. SECURITY MEASURES……13

5.1 SOCIAL NETWORK SCAMS AND COUNTERMEASURE……13

5.2 SECURITY IN CLOUD COMPUTING……13

5.3 MOBILE DEVICE DATA SECURITY……15

5.4 SOCIAL DATA LOSS AND COUNTERMEASURES……15

5.4.1 Security Policy……16

5.4.2 Preventive Measures……16

6. SECURE PROTOCOLS……18

6.1 LAYER SECURITY……18

6.1.1 Secure Sockets Layer (SSL)……18

6.1.2 Transport Layer Security (TLS) ……20

6.1.3 Drawbacks of SSL and TLS……20

6.2 SET (Secure Electronic Transaction) ……21

6.3 3D SECURE PROTOCOLS……22

6.3.1 Advantages of 3D Secure……23

6.3.2 Drawbacks of 3D Secure……23

7. CONCLUSION……25

BIBLIOGRAPHY……26

APPENDIX……30

Author	Anup G.C.	Year	2013
Subject of thesis	Credit Card Security		
Number of pages	36+2		

Credit Card is a widely used electronic chip for easy transactions. The main purpose of the report was to show the security measures of transaction by credit cards. The purpose was to give information about credit cards and how they were introduced. The thesis reportcontained the types of card theft with examples and sited the various protocols used for online transactions. The aim of the thesis project was to conclude whether the card security provided by the banks is safe enough.

The thesis report contained information about many online resources as well as liable books. Many news articles were also considered while writing the report for the card theft records.

The thesis report described both the positive and negative aspects of the protocols used for card securities. Result showed that misuse and complicated processes of protocols has led the identity theft to transactions. To conclude, although many security measures are implemented for the secure transactions, credit card fraud activities are happening in a weekly basis.

Key words secure protocols, SSL, SET, bank theft, EMV

1 INTRODUCTION

In today's world money has made life much easier in terms of transaction and in exchange of ecommerce market via different ways. People buy something, sell something or want to pay for something. In all purchasingprocess money has been the good way in payment issues. Daily lifespan from waking up in the morning to the sleeping time, many personal money transactions can be seen. To save much time people use cards issued by the related banks. It might be an ATM card, a debit card or a credit card. They are all issued to users as a system of payment. Among them Debit card provides the cardholder electronic access to users bank accounts at their own financial institution having their stored value and can withdraw funds from a payee's designated bank account. However,Credit cards are made for emergency payment electronic service to pay for goods based on the holder's promise to pay for them.

Credit card limits are varied by the credit card issuer followed by the bank accounts and debt. Certain amount of interest is also charged depending upon the interest making it different from charge card and cash card. The transactions are done by the successful contact and verification between Credit card and merchant's electronic device. Furthermore, the transactions could also happen with the online access or over the phone known as Card Not Present (CNP) transactions.

With purchasing services considering the electronic payment system, the credit card saves more time than cash transactions. Credit card allows small short term loans to be quickly made to a costumer as well as online and offline transactions with nominal annual fee. Credit card allows immediate transfer of funds, easy to carry, handle and manage.

Credit cards have been used highly in the world which increases the probability of theft incidents.Thus, this report explains the various techniques that are used for safe electronic transaction and credit card payment events to reduce the fraudulent acts and to get the support of consumer. The author presents the means of security during the presence of card (EMV) like using

the card in nearby shopping complex. More details can be found about security protocols given to the transactions like Transfer Layer Security(TLS), Secure Electronic Transactions(SET) and 3D Secure where cards are not present such as online internet shopping.

2 CONCEPTS

2.1 History of Credit Cards

If the history is studied, people have swapped goods in the exchange of gifts in markets where a commonly shared system of tokens are more convenient.Goods were exchanged in markets including precious metals, livestock and sacks of cereal grain and so on.Some conditions where people have nothing to exchange, time banking was introduced. Time banking is a process of exchanging services that values units of time as currency. Time banking was always valued at an hour's worth of any person's labor and can be paid with the same amount of work for other that has worked for him. This was first introduced as time credit in the UK and time dollar in the USA. (Woolsey−Gerson 2009; Carr 2010.)

Banks were considered as a secure way of storing funds. To compete the world with reference in time management and easy access, many advanced payment technologies have brought in use. Among them one is the payment system with electronic cards. The card holds the infrastructure of computer networks that are highly reliable to Automatic Teller machines (ATMs) and POS terminals having powerful mainframe computers of financial institutions. They are mainly known as magnetic stripe cards and ICCs having chips inside of the card. The card holds the action of users performing money withdrawal and financial account related to the card holder in terms of bank network. For example, a user wants to withdraw 50 euros from the nearest ATM machine urgently. Here he first inserts his card in the machine and he needs to prove his identity with the PIN number or security code given to him. With the proper combination a link is establishedbetween the user's account and the bank's financial network. The user will get the approval or denial of the withdrawal according to the funds available in his account. With the same mechanism of transferring and receiving funds, online access payment control also came in use with the help of the Internet world. Online payments are the easier way in purchasing goods and transferring funds in the online market.(Woolsey−Gerson 2009; Carr 2010.)

Fraud acts were increasing along with the introduction of advanced payment systems. Thus many security measures were applied for the access of transactions especially in online world. Within the same purpose, in 2004, the major credit card companies got together to start a common Payment Card Industry Data Security Standard (PCI DSS). PCI DSS is an open global forum security Standards council looking for the development and enhancing security acts to implement the security for data protection. The company was launched in 2006 and has five founding global brands as American Express, Discover Financial Services, JCB international, MasterCard Worldwide and Visa Inc. Another security measures as establishing a basic firewall security allows the protection from storing credit card numbers and information in the open browsers. Strict law for the companies that takes online payment access and strict fines for non-compliance to the amount tens, hundreds or thousands of dollars to put much small organization out of business. Even harsher treatment to the companies storing cards data when the system is hacked and information's are leaked.(Woolsey−Gerson 2009; Carr 2010.)

Apart from that many security measures were applied like PAN truncation that does not displays full number on the receipt, Tokenization that does not store full card details in the computer system of business networks, geolocation validation performing IP address, fraud detection preventing software's, firewalls, blocking cards in terms of lost or closing account, multifactor authentication for bigger transactions, out of band authentication and so on. With these all majors of security, consumer's money is secured by funds that were deposited and a reliable source as bank to hold the deposited money in confidential information. Thus, use of cards has been the easiest and secured means of money transactions giving a lot benefits to the consumer. (Woolsey−Gerson 2009; Carr 2010.)

2.2Bank Cards

2.2.1 Debit and Credit Cards

Bank cards are the cards issued by the banks in order to get various payment services from the funding accounts. Early bank cards were made of celluloid plastic, then metal and fiber, then paper, and are now mostly

polyvinyl chloride (PVC) plastic. They are connected with the ICC chip installed within it to the banking network and to the related outcomes like the machines available in payment stores, ATM machines and so on. They can be swiped at stores and enables to buy things without the cash which means they are easy access for the funding transactions. (Wikipedia Foundation Inc. 2013c)

Mainly in personal finance, bank cards like debit cards and credit cards are widely used all over the world. Among them, debit card is a card mainly known as prepaid card. Here, the card holders can withdraw the amount of transactions only from his/her stored funding account in the bank. But on the other side credit card allows users to purchase the items and billed monthly in correspond with his/her monthly expense. In another word credit card can be also considered as bank card. The comparison is described in Table 1 in appendix 1. (Diffen 2013.)

2.2.2 Working Mechanism

Several parties like namely, issuer, cardholder, the merchant, card association and settlement bank plays special role in the working mechanism of bank cards. Here issuer is known as a licensed financial institution that issues payment card and is responsible for the authorization requests. Cards are developed according to banks authorization using cryptographic ICC chips and PIN code security. The issuer host acts as a computing system that can access the cardholder accounts database and represents the issuer during the authorization, clearing and settlement. As the card is inserted in the payment card brands such as ATM machines of POS terminals in shop, a link is established by the provided network connected end to end between issuing and acquiring financial institutions. After the matching of identity confirmation between users and the bank account information payment methods are confirmed. (Cristian 2002.)

3 OCCURRENCE OF BANK THEFT

3.1 Identity Theft

As credit cards are being widely used all over the world, there is also a wide ranging term for theft and fraud incidents. To obtain unauthorized funds or transactions, credit card fraud incidents have been happening which is also known as identity theft. If we see the overall identity theft records, over 0.1% of all card transactions have been resulted as credit card fraud act. Apart from that 99.9% transactions have been countered as secure. Many security measures have been applied in the payment system and to manipulate the false transactions. Due to which it is taken as the reliable source of transactions and easy way of getting and taking personal money access.(Wikipedia Foundation Inc. 2013b.)

As a small example of cyber card attacks, most of the time when we swipe our card and punch the PIN details in stores like gas station or grocery, we are vulnerable to cyber pickpockets. Criminals uses their many techniques in collecting the information from the card like by double swiping or tapping the terminal phone line, PIN numbers(by recording through a camera, tapping the terminal or just by watching). Bank card identity theft also can be occurred in two ways as application fraud and account take over. Application fraud happens by opening an account in someone else's name with the fake documents and without authorization. Here criminals might try to gather the information by stealing documents or by creating fake documents.Account takeover occurs when a criminal completely takes over another person's account. Here first the criminal gathers the required personal information of the victim and then he contacts the card issuer to send the information in the verified email or to the related address. (Wikipedia Foundation Inc. 2013b.)

As an example for identity theft, some fraudulent charges were seen on a person's debit and credit card totaling around $1500 each in Tokyo, Japan (City data forum 2009). Another example as eighteen people have been charged in New Jersey being a part of a massive international fraud involving thousands of false identities, fraudulent documents, doctored credit reports

and more than $200 million in confirmed losses. FBI Special Agent James Simpson said in court records.(Katersky 2013.)

3.2 Stealing Cards

Wallet being stolen or missing you bag in some public area are the common news we can hear all over the city. The wallet you are carrying might have important materials like bank cards. Thus, false transactions are found to be happening by those stolen cards and many people are recorded to be victim from this cause. The criminal uses stolen cards claiming their own. Mainly it's been used as no-PIN that allows criminals to purchase the items without knowing the PIN details from the stolen card. This is also applicable for the online transactions where only name of the card holder, account number, expiration date and verification code behind the card is needed.

If the history is studied, many stolen credit cards and criminals are recorded in the news. In August 2009 Gonzalez was also indicted for the biggest known credit card theft to date — information from more than 130 million credit and debit cards was stolen at Heartland Payment systems, retailers 7-Eleven and Hannaford brothers, and two unidentified companies (Wise Accounts 2013). On the other hand in Washington DC, Russian cyber crook was sent to 7 years federal prison for trafficking stolen credit and debit cards. According to FBI, he was in possession to have more than 2.5 million stolen debit and credit card numbers. The record says that 45.6 million credit card details were exposed in a gap from July 2005 to the January 2007 through the systems at TJX Companies. Here Albert Gonzalez is accused of being the group leader for the thefts(Wise Accounts 2013). Furthermore, around 2 dozens thieves got away with $30,000 after making 203 transactions at 23 different bank machines with 79 bogus cards in Montreal area. The RCMP says that the incidents have been happening multiple times each week. Other than that, an investigation (Citibank Complaint) by FBI cybercrime agent Albert Murray shows two men made hundreds of fraudulent withdraws from New York City ATMs, getting $750,000.(Buck 2013.)

3.3 Phishing

Phishing is an act to get the required personal information with the forgery act of websites and phone calls. The act might lead to the leakage of username, passwords and credit card informations. In simple words, phishing is an email fraud method where the perpetrator sends out legitimate looking email to receive personal and financial information about the victims. They are mainly seemed to be happening from the online paying websites like PayPal, eBay, MSN, Yahoo, BestBuy, Amazon, and so on. Many fake websites are created for these acts that look like the original trustworthy pages with official logos asking personal identification and card information's that are sent to criminals email account. These leads to the wide range identity theft. Thus for such kind of reason Federal Trade Commission (FTC) was formed which warns users to be suspicious of any official looking email message that asks for updates on personal or financial information and urges recipients to go directly to the organization's web site to find out whether the request is legitimate.(Rouse 2007.)

The following are the two examples of the famous attacks recorded.
It has been estimated that in 1 year (May 2004 and May 2005) more than 1.2 million users in the US suffered losses caused by phishing to the amount of approximately US$929 million.Before the Federal Trade Commission (FTC), for a small example, a 17 year old boy sent out message saying there had been a billing problem giving AOL logos and contained legitimate links. Somehow they were taken to a spoofed AOL webpage asking personal details like personal information, credit card details, personal identification numbers, social security numbers, personal status, account numbers, passwords for login options, and so on. (Rouse 2007.)

3.4 Breaking Into Server

Breaking into servers is known as the wide range of data loss and huge loss of money. This kind of attacks are mainly done in a pair or in a group. They simply hack over the server and get all the information. Let's say if somebody hacks the server of bank and gets all the information of customers account and credit card details, false transactions can happen in a huge amount.As a

recorded news, In June 2013 New Jersey, eight members from an alleged international cyber ring hacked in to computer of major financial institutions and tried to seal $15 million dollars from the customer accounts (Buck 2013).

To some extent on May 2011, due to weak security environment designed for credit card database, online entertainment PC games network was hacked in which 77 million customers personal details were lost. It dropped the share price of Sony by 4% (JUCC 2013). Other than that, on March 2011, Epilson exposed names and emails of millions of customers' stores in more than 108 retail stores and in addition several huge financial firms like CitiGroup Inc. and the nonprofit educational organization, College Board (Amerding 2012).Furthermore, after the Antisec branch of Anonymous hacked into security think tank Forecasting, it is claimed that the theft was 200GB worth of data including the emails and clients' credit card information. Days after the hack, the group published 860,000 email addresses and 75,000 unencrypted credit card numbers on the web. It is said that between December 6, 2011 and February 2012 at least $700,000 worth of unauthorized charges were made to credit card accounts. (Kerr 2012.)

3.5 False Transaction By Merchant

It is impossible to say that all the merchants over the businesses are liable and honest. If the fraudulent thoughts come to their mind, merchants are the real criminals that consumer should be aware of. The machines they are using and transactions they are making can be something else than they are supposed to be. Some reported false transactions are cited as an example. For example, Waiters in about 40 restaurants in New York quietly recorded customers' credit cards information and passed it to the people who make the use of it to have more than 3 million dollar worth of illegal purchases (AP 2009). In Canada, Mark Wong ordered a sandwich and fries at a Richmond McDonald's and was charged $500 when the bill was supposed to be less than $10. Within the same fraud act, bank card fraud has reached doubling the quantity in past 3 years in Canada having $100 million of loss in 2006. (Jones 2013.)

4 EUROPAY, MASTERCARD AND VISA (EMV)

4.1 Working Mechanism

Europay, MasterCard and Visa (EMV) is a new standard in the evolution of bank cards. EMV has turned the previous typical magnetic stripes cards to a technological devices chip cards. According to the statistics more than 80 countries has been adopted EMV and more than 1.5 billion cards has been issued. EMV stands for Euro pay, MasterCard and Visa. In this technological World everything is unsafe, fraud and counterfeit is increasing day by day. People wanted more security and searching for the secure way for bank transaction .EMV sets the global standard for operation of chip cards, point-of-sale terminals, ATMS and so on. EMV chip cards contain embedded microprocessors that provide strong transaction security features and other application capabilities that are not possible with traditional magnetic stripe cards. EMV has unique element present in the card because of which it is not possible to use the stolen card without its presence. EMV technology have made people's everyday banking life more safer, secure and reduce fraud resulting from counterfeit, lost and stolen cards (Smart Card Alliance 2013.)

Figure 1. EMV payment card (Jeff 2013).

EMV payment cards are known most to take the transactions when the card is present with the card holder. With the access of card and any card acceptance device, safe transactions are made. Depending on the connection to the device two technologies are defined. (Jeff 2013.)

4.1.1 EMV Contact

EMV is secured because of card authentication, protecting against counterfeit cards, cardholder verification and transaction authorization. Payment information in a secure chip rather than on a magnetic stripe and the personalization of EMV cards are done using issuer-specific keys. EMV also provides interoperability with the global payments infrastructure–consumers with EMV chip payment cards can use their card on any EMV-compatible payment terminal. The fold square seen in the front face of the card is known as the card's contact. An embedded microprocessor chip can be found behind the gold contact plate. When in use the card is inserted into a card acceptance device and the contact allows the chip to connect to the reader. The connection then allows exchanging the data and verification of the correct user with safe transactions. This is known as contact chip card technology. (Jeff 2013.)

4.1.2 Contactless Payment Cards

In another hand of chip card technology, contactless chip cards are worked holding within a couple of inches of a contactless capable reader. Here, the reader energizes the chip embedded in the card and allows exchange of data by radio frequency without the card ever leaving the cardholder's possession. It's been also said that contactless payment cards are 53 percent faster than a magnetic stripe card and are 63 percent faster than using cash. (Jeff 2013.)

Figure 2.Contactless Payment (Contactless payment 2013).

It's not necessary to put the PIN details to the device as the radio wave between the card and device can make the transactions. But for security purpose and to make sure that the card belongs to the legal card holder time to time user will be prompted to enter their PIN. Each time a PIN used it confirms that the cardholder is still in possession of their card. (Contactless Payment 2013)

4.2 BENEFITS OF EMV

Due to the EMV payment system, more security has come against the credit card fraud that rely only on data encoded in a magnetic stripe on the back of the card. Within this, the chip provides its authenticity in an offline environment and makes the payment safe. It can be used to secure online payment and protect cardholders, merchants and issuers against fraud through a transaction unique online cryptogram. It supports enhanced cardholder verification methods and stores more information than the magnetic stripe cards. Thus consumer feels comfortable on using chip technology methods in payment and has gained their trust towards it. (Jeff 2013.)

5 SECURITY MEASURES

5.1Social Network Measures and Counter-Measures

With the regular consequences happening and for the easy income lots of people are changing their thought into criminal mind act specially the one who are good known to the computer databases and professional workers that are not satisfied with the company. This leads to the heavy loss of personal identification within a clean shot. In many case social networks based scams are also the most rapid growth in online attacks. For example in the mid of 2011 a victim received a message on Facebook from “friend” inviting him to view a video. Here the users were requested to update their computer by downloading unknown software and it lead to the active data transfer and steal information from the user’s computer. Due to the lack of systematic monitoring and test before production launch many application vulnerabilities happening everyday especially in the web application having weak securities. (JUCC 2013.)

Data shows that almost 20% of all Facebook users are active targets of malware. It works as a quick translation of cross-site scripting (XSS) and cross-site request forgery (CSRF) vulnerabilities and leads into massive security outbreaks. To keep our computer’s data in a protected way from social scams, best way is to avoid any social networking postings from unknown sources and the use of malware-detection applications such as “SafeGo”. It scans account profile for any suspicious links and notifies when any chances of threats are detected. (JUCC 2013.)

5.2 Security in Cloud Computing

It is seen in a survey that providers of cloud computing do not view the security of their cloud services as a competitive advantage. They are good in providing the services to the consumers but in terms of security it seems the providers haven’t considered much. Due to weak security and due to the lack of proper action on security lots of threat are encountered everyday like data breaches, data loss, account hijacking, insecure APIs, denial of service, malicious insiders, abuse of cloud services, insuffient due diligence, shared technology issues and so on. These all threats are indirectly related to the

easy access of money stealing personal identities. And Gartner predicts that public cloud services will reach $206.6 billion in 2016 where the service is counted as $91.4 billion. The result shows more than 120% of total increment within 5 years of time. But if the security of cloud computing goes the same way business will be uncomfortable with data security and much growth as planned won't see its proper direction. (JUCC ;Gonsalves 2013.)

Seeing the loss in huge amount of money and the possibilities of ending up the mutual understanding relation between businesses, cloud computing provides should keep their eyes on the security. Many countermeasures and controls can be applied to make the cloud computing secure. (Wikipedia Foundation Inc. 2013a.)

Deterrent Controlsshows much of like warning sign during attacks in the system. These controls do not reduce or crash the application of attackers but gives information to the providers or users about something is going wrong in the system. Preventive controls might be applied to manage the vulnerabilities and to upgrade the strength of the system. The system works in reducing the vulnerable acts in the system. These controls are placed to cover the attack and prevent the system from any damages. Thus, known as the preventive controls to prevent the violation to the system's security. Corrective Controlscan also be used in reducing the terms of violation in system but unlike the preventive controls, they always act like an attack is occurring in the system.Detective controls work as the naming of detective. They are always active in the systems to figure out the attacks to be happening in the system. During the attacks the system gives signal to the preventive controls and corrective controls to address the issue.(Wikipedia Foundation Inc. 2013a.)

Apartment from that many terms should be researched in order to give physical and personnel security, application security, privacies and legal issues correspondent to the computing. In some extinct case of disaster in the system an alternative means of application should be transformed to continue the business and data recovery to stop the flow of data loss.(Wikipedia Foundation Inc. 2013a.)

5.3 Mobile Device Data Security

Installation of operating systems and applications from the unknown source in mobile phone leads to the easy access of data loss. The recorded data shows that in March 2011, more than 50 third-party applications on Google's official Android Market are discovered to contain a Trojan called Droid Dream. In use of such kind of unknown source applications, Trojan or some other viruses are released which attracts the saved information from the users Smartphone and transfers to the hackers network. In this way if users have put all the personal information including Bank information and credit card details then turns into a heavy loss of transactions. (JUCC 2013.)

Thus it is always recommended from the mobile networks to avoid installation of applications and operating systems from the unknown source like for example installing jail broken iOS for apple devices. Also good way to prevent from those viruses is to install antivirus applications in the mobile phones which detects and kills the viruses or give warnings.(JUCC 2013.)

5.4 Social Data Loss and Counter-Measures

Leaving social network scams, mobile scams and weak cloud computing scams there are other many ways where data's are found to be stolen. For an instance and example shown above to the violence act of 17 year old boy claiming official executive and sending original looking non official emails that leads to the leakage of important information's.(JUCC 2013.)

In current situation most of the fraudulent acts are happening due to wrong authority access. Criminal pretends to be the authority of someone and flashes the information that is stolen from the victims where he gets the access to the credit cards or to the bank account and transactions. Thus it is very important to play several roles regarding security policy, personal act, more information about preventive and responsive measures and so on. (JUCC 2013.)

5.4.1 Security policy

Lots of money transactions software and online payments sites are available in the internet. To give a worldwide access and to get users from all over the world the IT management team or software providers should provide secured applications. The management should act in a way that the criminal and fraudulent theft is encountered almost to 0%. Some general policies can be maintained to make the money transactions secure. Software's should be built up in where strong authentication should be required for the transaction. Applications should have a general guidance in the beginning which gives the general information about the software.Help and support in harsh situations. Small information about the infrastructure security should be discussed to win the reliability of users. For internal security IT teams should always stay standby in order to prevent data loss during application crash. Disposal and re-allocation of computing resources better to maintain proper procedures. Backup applications should be used to detect the smell of identity theft and to keep the work running during the damage of software. Management and softwareapplications should be updated in a while.IT security officer must be kept up-to-date with latest security and hacking techniques.Legal terms should be issued in terms of violence.(JUCC 2013.)

5.4.2 Preventive measures

Before using and kind of applications or taking any kind of steps in terms of transactions, users should have at least the basic information of how the system works and what could be the possible outcome. Some possible preventive measures should be played to be safe from scams like should avoid replying emails from the unknown source or verify the source before responding. User must be ready to act in suspicious calls to generate the verified information of the cause. Clean records of electronic storage media and shared documents should be made.User should avoid the use of recommended websites from the unknown source or verify the identity of the websites with website certificate and domain name.Do not USB device from unknown source or scan before using any external devices.Get general information before using or taking any steps that is related to any transaction measures.Check whether the security controls are strong enough in your

computer and smart devices.Make the informative means password or firewall protected and install detection software’s which gives you alert warnings in theft act.(JUCC 2013.)

6 SECURE PROTOCOLS

6.1 Layer Security

Due to the various threats and fraudulent act, security layer was an important task to use the confidential online transactions and internet use in a secure and authenticated way between buyers and merchants. This might varies by the differences in public key and symmetric key encryption with respect to number of parties having private keys and certificate. Somehow consumers trust was to be gained by showing the secure means of way while purchasing goods. Thus the following security layers were introduced and were brought in use. (Entrust 2007.)

6.1.1 Secure Sockets Layer (SSL)

Secure Sockets Layer was originated by Netscape. SSL is used to provide secure means of surfing and communication purposes in all over the internet. The protocol uses single private key for the encryption in data communication. SSL works on a program based layer between HTTP (Hyper Text Transfer Protocol) and TCP (Transfer Layer Protocol). The word “Sockets” in this layer refers to the process of data passing between clients and servers within the network or between the program layers along the same computers. The layer used both public and private key encryption from RSA and also has a digital certificate.(Entrust 2007.)

SSL layer mainly works on two method security as encryption and identification. Encryption is something like hiding what is sent from one computer to another and giving a secure transmission. With this, the information sent with the submitting button will take the message without any leakage. Identification is to make sure that the computer you are monitoring is the one you trust and was supposed to communicate with. Identification works with the convention of digital certificates. These certificates are known for the electronic files which help to identify people and their main source over secure communications and transactions in internet.(Entrust 2007.)

When clients or users wants to make a transaction and connects to a SSL protected website (website URL starting with https), the website authenticates the identity using the SSL certificate to the client with a

cryptographic proof that the system has the associated private key. Then the client verifies whether to trust the certificate by the signature and if the website seems to have a trust worthy certificate, no trust dialogs are presented and the connection is a secure way for transaction.Now the user of client can share the credit card details to the merchant with secure internet transmission and the merchant appeals for the credit card distributor with the verification certificate and details of his/her clients and get his/her money. After the money transaction completes, the credit card issuer again bills with the amount of shopping covered to the client. This was the primitive way of securely transactions and was also costly to perform several processes.(Shamos 2004.)

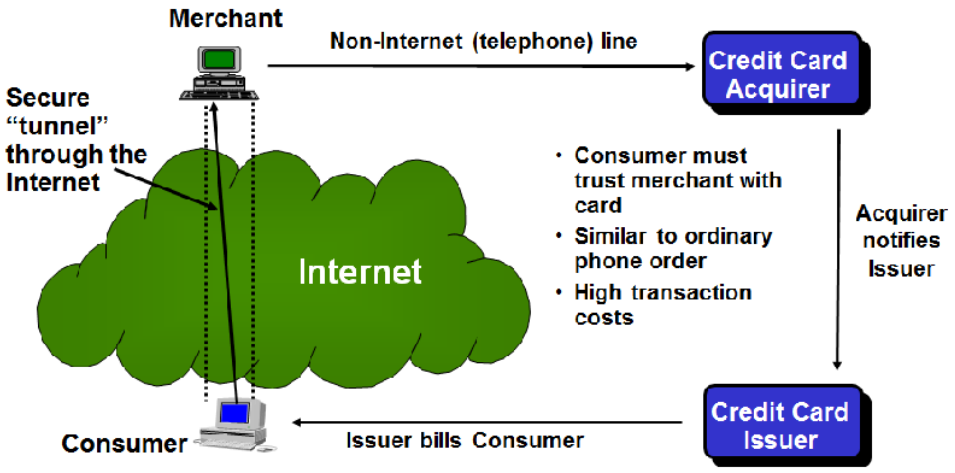

Figure 3.Electronic Payment Systems (Shamos 2004).

And if the dialogue box appears or website browser says that the certificate is untrusted, the box means the way for transaction is not secure and isn't signed by a trusted root certificate to a trusted root certificate. (Entrust 2007)

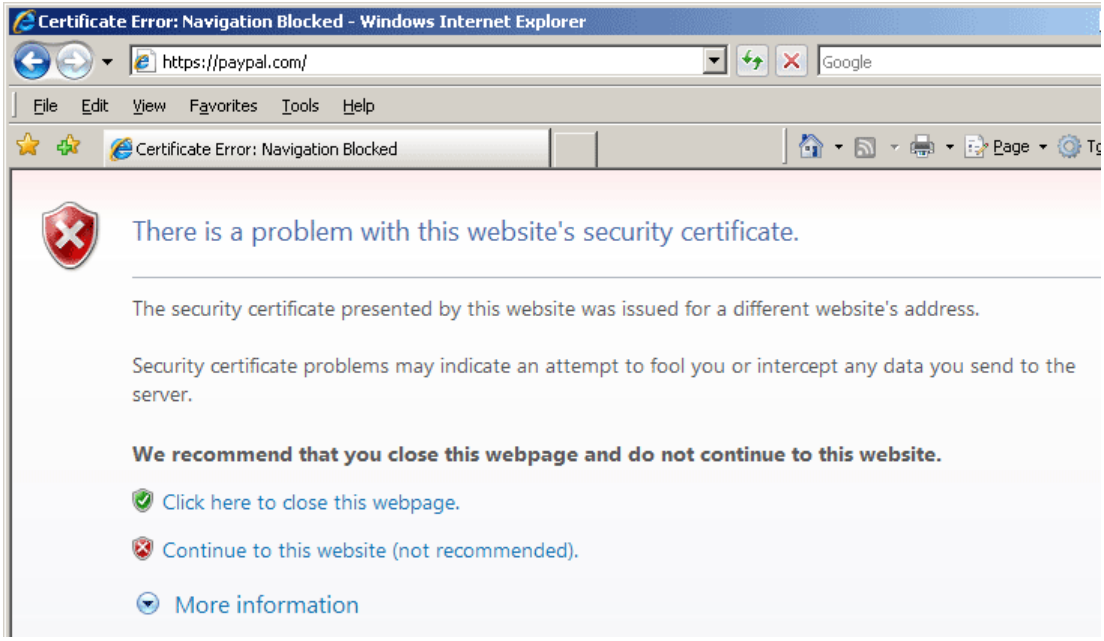

Figure 4.Warning Dialog box, Internet Explorer 7 (Entrust 2007).

6.1.2 Transport Layer Security (TLS)

TLS known for Transport Layer Security are also used all over the internet for the security purpose. TLS works almost same as SSL but is originated as IETF (Internet Engineering Task Force) version of SSL in 1996 after the SSL version 3.0, but just due to the cryptography TLS is differed from SSL. And somehow browsers understand both SSL and TLS. Main idea to operate TLS is to reduce the network activity and give efficient security layers with separate layers and handshaking protocols. (Instabill high risk 2013.)

6.1.3 Drawbacks of SSL and TLS

SSL and TLS protocols are known for common secure protocols all over the world despite some major draw backs. Transactions seem to become slow and processing becomes sluggish without SSL's accelerators.Because of slow SSL processing, customers might close the browser and go to another web shop.Web servers are unable to handle much pressure of load at times.Some sensitive information is not transmitted properly in time leading to the security breach. (Instabill high risk 2013.)

6.2 Secure Electronic Transaction (SET)

SSL and TLS layers are found to be widely used today on the internet. But it has also introduced huge risks in the online market. The saying is true that the data sent through SSL or TLS is encrypted and no other party than consumers and merchants can get the credit card details. But some merchants were and might be dishonest with the external use of card details; some might be just a hacker who makes illegal website with XYZ corp. and collect card details for personal use. Thus with a promise for fully secure transactions Visa, MasterCard and a consortium of 11 technology, Secure Electronic Transaction (SET) was introduced. The main purpose is to provide confidentiality of information, ensure the integrity of payment instructions for goods and services order data and authenticate both the cardholder and the merchant. Four entities Cardholder (customer), Merchant (web server), Merchant's bank and Issuer (cardholder's bank) plays the main role in this security layer.(Li 2001.)

In case of account transaction through internet, first cardholders, merchants, and acquirers are supposed to have a digital certificate followed by the related organizations and should have registered with the Certificate Authority (CA). Then, credit card details punched by the client are redirected to credit card acquirer via internet in reference to merchant. Here, merchant won't be able to see card details but money followed by the client will be transferred in merchant's account. This way card details are not published to the third party between bank and the user which seems the better and safer way of transaction reducing the identity theft and fraud acts.(Shamos 2004.)

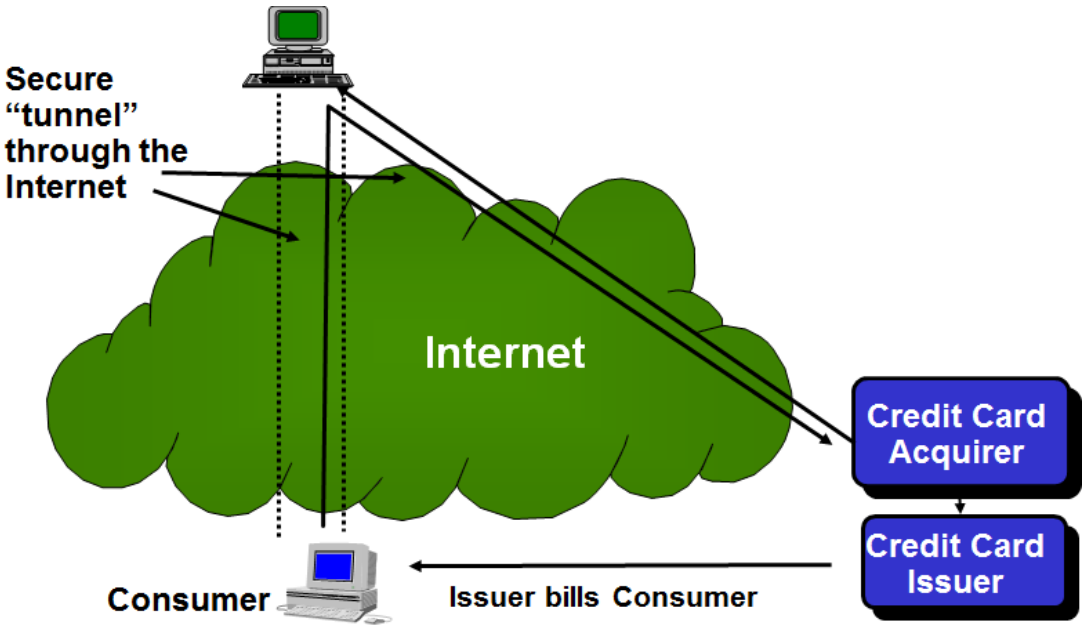

Figure 5.Secure Electronic Transaction (Shamos 2004)

6.3 3D Secure Protocols

3D secure is a latest technical security measure developed by Visa and MasterCard to provide further secure pathway on online transactions over the internet during CNP (Cardholder Not Present). MasterCard gave their name as "MasterCard Secure Code" and Visa named their as "Verified by Visa" and also American Express added the protocol as a "Safe Key" for the web shops to have online transactions. The protocol is an XML based protocol that includes the issues that affect the consumer with bigger protection area for phishing and a liable source in online transactions. (ZMS 2009.)

First the cardholder is provided with a personal pin or password to use while doing the online transactions. This ensures that the shopper who they claim to be are the real one and the cardholder's information is protected from fraudulent use on the internet. Once the consumer is registered with the security pin or password, every time he wants to make a purchase a pop up

window opens and the additional security question is needed to be typed. Then the given answer or password will be quickly confirmed by the card issuer and the items can be purchased. So the main entities here are cardholder, card issuer, payment association and merchant with his acquirer.(ZMS 2009.)

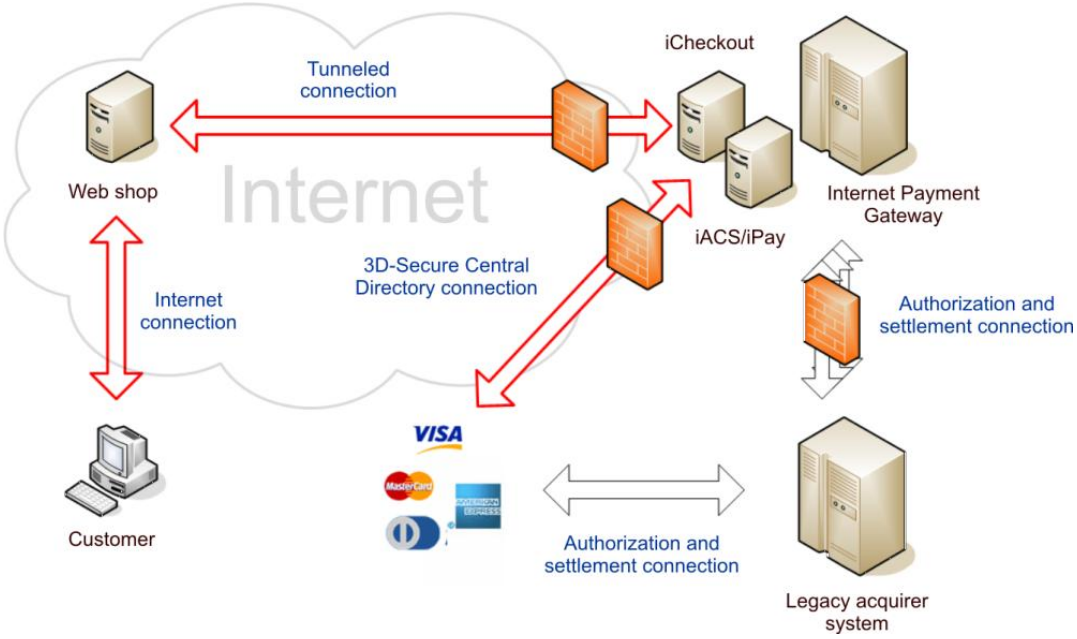

Figure 6.Checkout process with 3D Secure (ZMS 2009).

6.3.1 Advantages of 3D secure

3D secure allows authentication technology in online validation of payments in CNP situations. With this technology lots of advantages are found during web shopping's. With this protocol misuse of cards and loss of payments are reduced. With the additional authentication process transferred payments are found to be protected. The liable source and confidence of customer has increased in sales. Merchants find the process a safe way to accept international cards. 3D secure has also provided better international transactions and offers better transactions using SSL encryption. (Instabill high risk 2013.)

6.3.2 Drawbacks of 3D secure

As a wide range of protection systems and the secure way for online shopping it is claimed that merchants should not consider 3D secure protocol

as a universal remedy for all kinds of online payment. The ecommerce web sites connect directly to a bank that performs the task with the person's password in the iframe and the transactions are completed with the verification of password. But the researcher claims that since there's no URL mentioned with the iframe and quite difficult to analyze whether the protocol is secure or not. (Kirk 2010.)

In another case, 3D allows setting and changing their password as they enroll with the system and the process is known as ADS (Activation During Shopping). ADS enrollment system asks for general information such as birth dates to confirm the setting of password and the researcher says that date of birth and general information of the consumer are easy to obtain. The situation might lead the hackers open way in changing the passwords and purchase their personal goods. People also claim that 3D secure protocol is vulnerable to phishing where fraudsters can use various emails to extract person's information and password. (Kirk 2010.)

Most of the online shopping users are also unlikely to read all the terms and conditions which means customers might end up paying for the bad transactions with their card and according to Murdoch he hasn't heard about however of a customer being held liable for a fraudulent 3D secure transaction. Some additional problems that are happening in 3D secure protocols. Security field added to the online form transactions have lowered the percentage of successful transactions which is an obstacle to purchase. Due to the lack of information about 3DS, customer closes their browsers leading to the loss in transactions. Banks offer customers with the list of one time codes for money transfers within bank use and these same codes are used for shopping also. Thus, the protocol is not good regarding the security issue. So, people carry codes with them often for easy access leading to the expose and leakage of codes. Protocols connect to unfamiliar domain names and causes extra delay or the application crashes. Passwords are often required and bigger chance for customers to forget which leads to a complicated process. Additional charged payment for using 3D secure protocol by the payment providers. (Kirk 2010.)

7 CONCLUSION

Credit cards are widely used all over the world via different means. Many people use the card to purchase products in shops and online market. The author has presented the importance of security while using credit cards. The occurrence of bank theft and fraud act with two conditions as Card Present (CP) and Card Not Present (CNP) were the main topics sited by the author.

Different technologies are used to prevent the scams. The various card thefts were discussed by giving examples. The report also shows the technologies that are used for securities and different protocols to prevent scams. For example Transfer Layer Security, Secure Electronic Transaction and 3D secure were explained. Within the technologies, the report also gave some information about the drawbacks and the preventive solutions. After the research and record of theft acts, the result can be seen that the use of cards is still not safe in many ways. Therefore, good preventive measures with proper theft scanning software should be introduced and implemented as soon as possible.

BIBLIOGRAPHY

Amerding, T 2012. The 15 worst data security breaches of the 21st century. Address http://www.csoonline.com/article/700263/the-15-worst-data-security-breaches-of-the-21st-century. Accessed 8 October 2013.

AP 2009. Waiters Attested in $3M. Address http://www.cbsnews.com/2100-201_162-2713680.html. 8 October 2013.

Buck, C. 2013. Cyberattacks on the rise as credit. Address http://www.sacbee.com/2013/06/17/5504045/cyberattacks-on-the-rise-as-credit.html. Accessed 8 October 2013.

Carr, D. 2010. Taking credit card security seriously. Address http://www.forbes.com/2010/05/17/security-paypal-pci-technology-business-survival-10-credit-card.html. Accessed 5 October 2013.

City data forum 2009.Tokyo credit card fraud. Address http://www.city-data.com/forum/asia/790212-tokyo-credit-card-fraud.html. Accessed 8 October 2013.

Contactless Payment 2013.Contactless payment in the UK. Address http://www.contactless-payment.co.uk/contactless-payment/. Accessed 01 November 2013.

Diffen 2013.Credit card vs. debit card. Address http://www.diffen.com/difference/Credit_Card_vs_Debit_Card#. Accessed 7 October 2013.

Drimer, S−Anderson,R−Bond, M 2013. Banking Security. Address http://www.cl.cam.ac.uk/~sjm217/talks/owasp13bankingsecurity.pdf. Accessed 08.10.2013.

Entrust 2007. Understanding Digital Certificates and SSL.Address http://www.entrust.net/ssl-certificates/how-does-ssl-work.htm Accessed on 22 October 2013.

Gonsalves, A 2013. The 9 top threats from cloud computing. Address http://readwrite.com/2013/03/04/9-top-threats-from-cloud-computing#awesm=~ojWtt6k7g5gHqP. Accessed 11 October 2013

Goodin, D. 2009. Heartland payment suspect. Address http://www.theregister.co.uk/2009/08/17/heartland_payment_suspect/. 8 October 2013.

Instabill high risk 2013. 3D secure and its advantages. Address http://www.instabill.com/articles/ecommerce-security-and-fraud-protection/3d-secure-and-its-advantages/. Accessed 23 October 2013.

Jeff 2013. EMV. Address http://merchantaccountroi.com/EMV/. Accessed 01 November 2013.

Jones, A. 2013.Famous Debit and Credit Fraud Cases. Address http://www.scribd.com/doc/131544009/Famous-Debit-and-Credit-Fraud-Cases. 8 October 2013.

Katersky, A 2013. Massive 200m credit card fraud. Address http://news.yahoo.com/massive-200m-credit-card-fraud-153836262--abc-news-topstories.html. 8 October 2013.

Kerr, D 2012. FBI says $700k charged in Anonymous' Stratford attack. Address http://news.cnet.com/8301-1009_3-57395944-83/fbi-says-$700k-charged-in-anonymous-stratfor-attack/. 8 October 2013.

Kirk, J 2010. Pc World. Address http://www.pcworld.com/article/187849/article.html. Accessed 23 October 2013.

JUCC 2013.Information Security-Trends and Countermeasures. Address http://www.istf.jucc.edu.hk/awareness_training/series_04/04_S1_Final.pdf. Accessed 10 October 2013.

Li, Y. 2001. Secure Electronic Transaction. Address http://people.dsv.su.se/~matei/courses/IK2001_SJE/li-wang_SET.pdf Accessed 22 October 2013.

PCI Security Standards Council 2013. History and About us. Address https://www.pcisecuritystandards.org/. Accessed 5 October 2013.

Radu, C 2002.Implementing Electronic card payment systems.Artech House, Norwood, MA, USA.

Rouse, M 2007. What is Phishing? Address: http://searchsecurity.techtarget.com/definition/phishing. Accessed 8 October 2013.

Shamos, M 2004.Electronic payment systems. Address http://euro.ecom.cmu.edu/program/courses/tcr763/ .Accessed on 18 October 2013.

Smart Card Alliance 2013. EMV: FAQ. Address http://www.smartcardalliance.org/pages/publications-emv-faq. Accessed 01 November 2013.

Wikipedia Foundation Inc 2013a.Cloud computing security. Address http://en.wikipedia.org/wiki/Cloud_computing_security. Accessed 11 October 2013.

─2013b Credit card fraud Countermeasures. Address http://en.wikipedia.org/wiki/Credit_card_fraud#Countermeasures. Accessed 7 October 2013.

─2013c. Debit Card. Address http://en.wikipedia.org/wiki/Debit_card. Accessed 2 October 2013.

Wise Accounts 2013. Who has a license to print money. Address http://wiseaccounts.biz/blog/who-has-a-license-to-print-money. Accessed on 26 November 2013.

Woolsey, B. − Gerson, E 2009. Credit cards history. Address http://www.creditcards.com/credit-card-news/credit-cards-history-1264.php. Accessed 04 October 2013.

ZMS 2009.iCheckout. Address http://www.zmsinfo.hr/Solutions/InternetAndCardNotPresentSolutions/iCheckout. Accessed 23 October 2013.

Appendix 1

Table 1. Comparison Charts of Credit and Debit Cards (Diffen 2013)

	Credit Card	**Debit Card**
Where money comes from	Borrowing money from a bank or financial institution. (Spending "other's" money)	Funds taken from the money that you have in your bank account. (Spendingyour "own" money)
Canbeused as:	Credit cardonly	Debit or credit card i.e., a debit card may be used without a PIN for certain types of transactions such as e-commerce.
Line of Credit:	Carries Line of Credit	No Line of Credit
PIN Number:	Usually not. However, some credit cards may provide PINs to allow consumers to withdraw money from ATMs just like debit cards. Such withdrawals are generally a bad idea because they carry high fees and interest rates.	PIN number provided, but not always asked to punch in.
Picture ID	Yes	No

	Credit Card	Debit Card
required before issuance:		
Interest:	If a credit card bill is not paid in full, interest is charged on outstanding balance and the interest rate is very high.	No interest is charged because no money is borrowed. Consumers own funds are used to make purchases.
Credit History:	Responsible credit card usage and payment can improve one's credit rating. Credit cards typically report account activity to at least one of the three major credit bureaus on a monthly basis.	Does not affect credit history.
Legal Liabilitylaws:	Strict. Consumer liability limit for credit card fraud is $50 if the credit card company is notified within 60 days in written since the fraudulent charges.	Lean. Consumer liability limit for debit card fraud is $50 if the bank is notified within two days of noticing the fraudulent charges.
Riskinvolved:	Low. Consumers are protected against unauthorized purchases as long as the fraud is reported in a timely manner. Consumers are not responsible for charges incurred in fraudulent	High, as they are attached to a bank account. A person does not need a PIN number to use a debit card and therefore can easily drain a person’s bank account, causing extreme problems.

	Credit Card	Debit Card
	transactions.	
Fraud:	Only problem is proving that someone else has used the card.	With a debit card the person has to figure out how to get their money back and if any checks bounced they are responsible for those as well.
Limit:	Credit line, which can be increased/decreased from the time of applying.	Equalsyouraccountlimit.
OverdrawFees:	Low. Some credit card companies allow overdrawing amount over the maximum credit line with a fee.	High "overdraft" fees. Possible to overdraw amount over the account limit
Connected to:	Need not be connected to any bank account.	Need to be connected with checking or savings account
Monthly Bill:	Yes	No
Offers protection and other benefits:	Often. For example, extended warranties on new products, or insurance on a rental car.	Sometimes. For example, extended warranties on new products, or insurance on a rental car.