CHAPTER 3

ANALYSIS OF VULNERABILITIES IN ATM TRANSACTIONS

3.1 ISSUES OF VULNERABILITIES:

The term vulnerability in computer system is showing the weakness or fault in a system which allows hacker or attacker to breach the reliability of that system for making gross misuse or abuse of the system or machine. Vulnerabilities may result from weak passwords, a computer virus or a script code. Vulnerability is Security holes/bugs or faults, defects, or programming errors. These may be exploited by unauthorized users to access computer networks or web servers from the Internet. The word “vulnerability” describes a problem, such as a programming bug or common configuration error that allows a system to for unauthorized access or to be attacked or broken into [41]. Indeed, finding vulnerabilities is a big part of the hacker/information security culture.

Security vulnerability is anything that offers a potential avenue of attack against a system, including from things like viruses, incorrectly-configured systems, and passwords written on sticky pads, and so on. It’s true that issues like these do increase the risk to a system. Vulnerabilities often result from the carelessness of a programmer, though they may have other causes. Vulnerability may allow an attacker to misuse an application through for example bypassing access control checks or executing commands on the system hosting the application.

“Security vulnerability is a flaw in a product that makes it infeasible – even when using the product properly —to prevent an attacker from usurping privileges on the user’s system, regulating its operation, compromising data on it, or assuming ungranted trust.”
Security vulnerabilities involve unintended weaknesses, by-design weaknesses may sometimes occur in a product, but these aren’t security vulnerabilities. Security vulnerabilities are a result of a problem in a product. Problems that result from adhering to imperfect but widely accepted standards are not security vulnerabilities. Security vulnerabilities involve a loss of control. That is, in order for a flaw to constitute security vulnerability, it must be possible for an attacker to compel the victim to submit to the attack despite reasonable efforts to avoid it. Every product has documentation that describes how it is intended to be used. In addition, best practice guides discuss reasonable and customary ways of using products. In order for a flaw to be security vulnerability, it must occur when the product is used in the expected, required, or reasonable way. Privilege elevation vulnerabilities involve supercilious illegal capabilities. Regulating a system’s operation is actually a special case of usurping privileges, but we’ve addressed it separately because of the importance of denial-of-service and similar attacks.

The ability to access data contrary to the owner’s or the administrator’s efforts constitutes a security vulnerability. Depending on the scenario, this could involve reading, adding, or modifying data. Data on a system includes information whose compromise poses a danger as a primary effect. Examples of data on a system include user data files, cryptographic key stores, etc. if it poses a danger at all, poses it as a secondary or tertiary effect. Examples include information about the logical structure of the system such as network topology, file locations, and so on. Many products enable the user to specify people or organizations that they trust, and regulate their actions accordingly. Flaws that enable an attacker to gain a level of trust the user didn’t grant constitute security vulnerabilities.

Vulnerability is anything running on a computer that could directly or indirectly lead to the compromise or breach of confidentiality, integrity, or availability of information or services anywhere on the network.

Confidentiality breach – it generates when unauthorized read access.

Integrity breach – it generates when unauthorized creation, modification, or deletion of files.

Availability breach – it generates when denial of service.
3.2 ATM VULNERABILITY:

In terms of Automated teller machine vulnerability, it mean weakness in the overall system which exploit the banking operation and allows an unauthorized user to have access to any other customers’ account and perform financial operation using Automated teller machine for transacting from any other customers’ account.

Here we are starting with some simple examples which indicate the variety of frauds that can be carried out without any great technical sophistication, and the bank operating procedures which let them happen. For the time being, I may consider that the magnetic strip on the customer’s card contains only his account number, and that his personal identification number (PIN) is derived by encrypting this account number and taking four digits from the result. Thus bank and the thief was only discovered because he suffered an attack of conscience and owned up.

Technical staff also steals client’s money, knowing that complaints will probably be ignored. At one bank in Scotland, a maintenance engineer fitted an Automated teller machine with a handheld computer, which recorded customers PINs and account numbers. He then made up counterfeit cards and looted their accounts. Most thefts by staff show up as phantom withdrawals at Automated teller machine in the victims’ neighborhood. English banks maintain that a computer security problem would result in a random distribution of transactions round the country, and as most disputed withdrawals happen near the customers’ home or place of work; these must be due to cardholder negligence. Thus the pattern of complaints which arises from thefts by their own staff only tends to reinforce the banks’ complacency about their systems. A simple but effective scam is a man was stand in Automated teller machine queues, observe customers’ PINs, pick up the discarded Automated teller machine tickets, copy the account numbers from the tickets to blank cards, and use these to loot the customers’ accounts. This trick had been used and reported several years at large number of places. These attacks worked because the banks printed full account number on the Automated teller machine ticket in older Automated teller machine and there was no cryptographic redundancy on the magnetic strip.

Another technical attack relies on the fact that most Automated teller machines networks do work on not encrypt or authenticate the encrypted authorization response to the Automated
teller machines. This means that an attacker has to record from print response from the bank to
the machine, and then keep on replaying it until the machine is empty. This technique, known as
jackpotting, is not limited to outsiders. These are some examples of frauds happened on
Automated teller machines. On study of these types of attacks further we can divide the
vulnerabilities in below defined categories.

**TYPES OF ATTACKS ON ATM:**

A physical attack involves conventional weapons directed against an Automated teller machine
and its users or its related transmission lines.

An electronic attack (EA) involves the use the power of electromagnetic energy as a weapon,
more commonly as an electromagnetic pulse (EMP) to overload computer circuitry, but also in
a less violent form, to insert a stream of malicious digital code directly into banks software or
local Automated teller machines operating system and its softwares’.

A computer network attack (CNA), usually involves malicious code used as a weapon to
infect enemy computers to exploit a weakness in software, in the system configuration, or in
the computer security practices of an bank server. Other forms of CAN are enabled when an
attacker uses stolen information to enter restricted computer systems [42].

**CAUSE OF VULNERABILITY OCCURRENCE :**

Banking system for financial transactions are highly secure as it developed with a lot of effort
and applied after various types of testing process but there may some lacking behind it which
makes it vulnerable. These causes are described below :

- The bank or the customer being cheated
- The faults in the machines, software and procedures
- Inadequacy or failure of security arrangements
- Unforeseen circumstances and accidents

This is caused when a customer or bank is being cheated with some Outsiders (strangers),
Insiders (employees) and Technicians (engineers, service providers).
1. OUTSIDERS OR STRANGERS

The ATM card and the PIN of ATM card are essential for breaking into an account. Fraud uses his cleverness in diverse methods to find out details of ATM card or card itself with PIN. The techniques for are getting AM card details and PIN may be:

(a) BY SHOULDER SURFING

‘Shoulder Surfing’ is a method for collecting the PIN by standing just behind the customer and overlooks over customer shoulder to watch key stroked by users and memorizes the PIN.

(b) SKIMMING

‘Skimming’ is collection of the PIN as well as the card details without the knowledge of the customer. Nothing abnormal is noticed by the customer in the Automated teller machine, but as ATM card of user goes through the card slot the attacker/thief/fraud receives the details of ATM card. This is achieved by pushing a ‘Skimmer’ into the Automated teller machine slot. Simmer having been placed at head reads the ATM card passes even before ATM card reaches the Automated teller machine card reader. The skimmer reads the data on the magnetic stripe on the card and transmits them into a storage device

(c) FALSE ATM FRONTS

Fraud Gangs prepare duplicate front panels of Automated teller machine and install the false Automated teller machine fronts with genuine in such a way that it is difficult to distinguish between from where False Automated teller machine Front has taken over a genuine Automated teller machine by covering with advertisements of the bank. It is almost impossible to make out that these parts are in addition to parts of Automated teller machine. False Automated teller machine Fronts does make any hindrances in working of the Automated teller machine i.e. the Automated teller machine works normally. The customers’ card passes first to SKIMMER as the front panel of Automated teller machine and transmits the ATM card details to a receiver

(d) FAKE ATMS

Fake Automated teller machines are installed at public places with bank stickers, hotline numbers etc., pasted all over to look like a genuine Automated teller machines but Fake Automated
teller machines connection to any network for actual working of Automated teller machine on internet. To deceive and look like genuine Automated teller machine are also designed to disburse some cash initially but Fake Automated teller machine stops disbursing after a few transactions. Later on, Fake Automated teller machines starts displaying that machine is having technical error or there is “No funds” available that that moment with the machine. After a few days, Fake Automated teller machines are removed. Frauds use Fake Automated teller machines only to know the details of ATM cards and PINs from the installed skimmer inside the Fake Automated teller machines and use it for cloning of cards and unauthorized access of user accounts.

(e) STEALING THE CARD

Frauds/thieves use a number tricks to steal the ATM card. May be nice looking gentleman may offer help to an elderly person or an uneducated card user in withdrawing the cash from Automated teller machines but after the transaction had taken place he replaced genuine ATM card with a fake ATM card. Employees may intercept the mails of employers or other employees to steal the cards. Jail Wardens or staff may steal ATM cards of their wards. Hospital employees or helpers in old age homes or hostel may steal ATM card of patients, ward or colleagues. Many person, in a hurry, move ahead without collecting the before the cards ejects, the persons around Automated teller machines notice it and make use of the active account for withdrawing cash. Some even change the PIN.

(f) SOCIAL ENGINEERING

A person posing to be as very responsible and making believe the other that he could be trusted for some help is the form of fraud called ‘Social Engineering’. Fraud convinces the innocent card owner that he can trusted on gentlemen looking person with his ATM card and PIN code. Fraud may be impersonation of bank officer, bank employee or police personnel or security staff. Some Frauds telephones a bank customer as Bank Officer intimating the ATM card holder that the bank has cancelled ATM card of that clients, which according to him has become defective card and is risk to security. He asks for the card but at the same time volunteers to get it collected. He says the old invalid PIN has also to be cancelled before issuing a new one and obtains the PIN. An accomplice collects the card. Second method
Analysis of Vulnerabilities in ATM Transactions

opted by him is he represents himself as an employee of the bank, canvassing for a contest for ATM card holders with huge sums as prize money. He gives them the form, which looks genuine. One of the conditions is that no box should be left empty, and it contains a box for the PIN. He then wants to verify the ATM card is genuine. He swipes them in his portable Skimmer. Third method is that fraud impersonating for a bank security officer rings up an ATM card holder and asks for his cooperation in nabbing a dishonest employee who is trying to steal funds from his account. To execute the trap he asks him to leave his card secretly under the door of the bank after closure of the bank. Next day, he informs him that the employee has been caught red handed and thanks him and tells him that his card is required as evidence and a fresh card would be issued to him and asks for PIN or pass word of ATM for its cancellation. Fraud having both the ATM card and PIN/password makes the transaction to siphon fund out of the account.

Some time a fraud poses like Police Officer and steals wallets by breaking into lockers in Social Clubs, Sports Club etc. He then rings up the card holder, identifies himself as a police officer, informs him that his ATM card and the wallet had been found with an arrested culprit. He says that ATM card will not be returned to him, but to the bank. He further says that a small formality needs to be complied with and the PIN has to be recorded in the files police investigation file and leaves a phone number saying that said phone number of Officer of the Police Station (actually his friend’s) and advises the ATM card owner to lodge a complaint. The second person(so called police officer) in name of formalities to be completed obtains PIN/password. Another method opted by fraud is, he himself appear as a well dressed senior police officer in uniform, with badges, gun etc, driving a big car with flash lights on, accosts elderly persons driving their car and, with his intimidating rough language checks belongings of car passenger and confiscates the ATM card and also obtains the PIN.

Yet in another way to obtain PIN/password is that fraud impersonating a senior officer of the super market lures a sales girl of the Super market there is huge cash incentive for her good work done, but she shall have work with confidentiality. He wants her ATM card and PIN so that incentive could be deposited into her account without the knowledge of other employees. The girl gives them ATM card and PIN/password.
(g) **LEBANESE LOOPS**

This was a method used in early version of Automated teller machine which had the practice of capturing the ATM card. The unauthorized person used to position a thin rigid plastic strip having long wires in the sides (Lebanese Loop), deep inside the Automated teller machine slot. ATM card holder unknowingly of fraud device in Automated teller machine inserts a card, but the ‘Loop’ prevents the normal functioning Automated teller machine and the machine stops. The culprit standing behind him asks card owner to retry by entering the PIN twice or thrice, but nothing happens. The culprit standing memorizes the PIN. After the card holder leaves, the culprit pulls out the strip with the help of the wires and obtains the ATM card.

(h) **HACKING THE ATM**

In certain banks, dedicated lines are used to connect the Automated teller machine to the host computer along with a separate dial-up line to the host for the use of maintenance engineers. Stealing the confidential number for the dial up line the hacker intrudes into the Automated teller machine circuit and converts some ATM cards into a Security Cards, which enables him to carry unauthorized transactions as bank official with ease.

(i) **JACKPOTTING**

It is a high-tech hacking method against Automated teller machines, by which hacker gains the control of Automated teller machines remotely over a network or open the front panel of Automated teller machines to plug a USB stick loaded with own software and gain the control of access of an Automated teller machines.

2. **INSIDERS (BANK EMPLOYEES)**

Automated teller machines cash containers are protected by a set of confidential combinations of pass words. Only the trusted members of the bank or the service providers have access over these confidential pass words. When the cash disappears mysteriously from Automated teller machines without any trace, it means that the combinations had been used with the connivance of the employees of bank or service provider, who has leaked out confidential pass word either due to negligence or force or convenience. It is also possible that person
required to refill the cash tray has himself stolen the money. Opportunities exist for collecting PINs and card details for the employees in the section dealing with ATM cards and PINs, and it is a matter of concern since these unauthorized transactions are carried out by none other than the bank employees or his collaborators.

3. TECHNICIANS (ENGINEERS, SERVICE PROVIDERS)

Automated teller machine technicians and service providers like cash fillers etc., are given separate passwords for conducting the Automated teller machines operations. These passwords are supposed to be activated only for the brief period of operation. There are instances where, due to negligence, the passwords were not deactivated or there was delay in deactivation of temporary pass words, and it resulted in the disappearance of cash from Automated teller machine.

4. BANK CUSTOMERS

It may be difficult to believe but it is true that some customers are also indulging in fraudulent activities when they notice any weakness in the system. During the 9/11 disaster of America, the banks, for humane reasons, decided to allow operations on Automated teller machines without their normal controls. Banks lost almost $ 15 million within a few days from the customers. In the ‘Transaction Reversal’ method, the customer removes some notes in the middle of the stack when the machine delivers a stack of notes i.e. customers opt not to cleanly collect all note and waits. The machine swallows the rest of the notes as unclaimed and records failure of transaction and thereby customer withdraws some notes (money) without any record and transactions in his/her account.

5. MODIFYING THE ATM

In Chinese a typical Automated teller machine theft has been reported by cutting the cash conveyor belt inside the Automated teller machine so that the undelivered cash falls within the machine which are collected by frauds no sooner the client leaves Automated teller machine hosing.
6. PROCESS TIME:

In certain Automated teller machines, the customers are required to swipe the ATM card and then remove it and thereafter customer has to hit a key to exit. If the key is not pressed, the Automated teller machine waits for 60 seconds before moving to standby position. Attacker knew this secret and used to transact as soon as the customer left, though the attacker may not succeed all the time as time had elapsed were successful many a time to make unauthorized transactions through Automated teller machine and looting the customer.

7. PHISHING:

Hackers obtains confidential details of bank password via email many time and it is known as Phishing technique. Hackers are successful sometimes in collecting ATM card PIN/pass words too. The customer believes the bogus e-mail looking to be genuine email from his banker’s asking for personal details, password/PIN etc.,

Various Security threats and abuses in Automated teller machine threats can be seen as potential violations of security with expected or unexpected harmful results, and exist because of vulnerability in a system. If an unauthorized user invades into a system he/she can destroy information, operating systems, and programs. They can disclose information or they can cause disruptions or interruptions i.e. damage systems, networks, organizations, institutions.

Classified of Sources of threats

**PHYSICAL:** which include natural disasters (fire, storm, water damage) and environmental conditions (dust, moister, humidity).

**TECHNICAL:** This is equipment or software failure e.g. A user apply for withdrawal in an Automated teller machine, the machine shows paid but the cash is not delivered.

**HUMAN:** Manipulation by human is the main source of communication breaches. It includes unauthorized users who wish to damage an Automated teller machine system, and authorized users who misuse the system either deliberately or accidentally. The human threats can be further categorized into two types
**INTERNAL:** Internal human threats are disgruntled employees, hackers, former employees, system administrators, LAN and data base administrators.

**EXTERNAL:** External human threats arise from commercial intelligence, government-sanctioned intelligence, vendors, manufacturers, kids looking for kicks, nosy reporters.

Theoretical, which includes the vulnerability of the algorithms, protocols, and mathematical tools used in the methods that they are implemented in the systems.

After analyzing various causes of generating vulnerabilities we can categorize the major three categories of various types of vulnerabilities of Automated teller machine. These are

(A) Physical Vulnerability

(B) Logical Vulnerability

(C) Communicational vulnerability

**A. PHYSICAL VULNERABILITY:**

Physical Vulnerability is related to Automated teller machine manufacturing defect or weakness, leaving scope for attackers or hackers to make physical changes in the manufacturing of machine. It may be some external attachment of external skimming devices to read the information and make a fake card or get the secure information using these external devices.

There are various attack methods available on an Automated teller machine by design, though there is a limited attack surface to exploit on an Automated teller machine; the ATM card reader, the keypad, the network or dial-up service, or the internal motherboard via USB or SD/CF card slot. There are basically two ways to conduct the attack, either through physically or remote means[43].

For the physical, ‘walk-up’ attack, one can simply identify the brand of the Automated teller machine, search online for the key that opens the outer shell of the Automated teller machine (used to expose the internal computer system and safe), and install their customized software (aka, rootkit) via the available SD/CF or USB slots. Using miner tempering with machine the attacker/hackers gain the physical access to the Automated teller machine.
Few Physical vulnerabilities are listed here as per our research content.

Card Skimming

PIN Spying

Pin interception

Card Trapping/Fishing

The Lebanese loop

Dispenser False Fronts

False ATM

Partial Withdrawals

Ram Raiding

Robberies

Safe cutting via frontal attacks etc.

The maximum number of Automated teller transactions comes from the ATM card, which may be obtained by frauds by any means for use of the card itself or cloned card made out of data of the original card and therefore it is essential to know the ATM card, the central point, playing chief role in vulnerability.

B. LOGICAL/OPERATIONAL VULNERABILITY:

Logical Vulnerability relates to software weaknesses where a software attack can easily be performed, it may be use of some virus attack or malware attack. Logical weaknesses are used to steal sensitive computer information and details of ATM cards. The information gathered is used for cloning a card i.e. for making a fake ATM card with all genuine information of the original ATM card.
Logical Vulnerabilities are listed below:

- Malware
-Viruses
- Jackpotting etc.

One type of logical vulnerability is the financial self-service scene of the Microsoft Windows operating system together with the use of IP networks, for communications services, has resulted in a considerable increase in security risks for Automatic Teller Machines as a direct consequence of the vulnerabilities which are common to open systems. At the same time, the world is experiencing a paradigm shift regarding cyber attacks[49]. Worldwide criminal gangs are currently pursuing low risk, sustainable sources of revenue and it is a matter of time before many criminals in modern countries join this emerging “criminal value chains” and target attractive assets in an organized manner. In this respect, undoubtedly an Automated teller machine network is an attractive asset. Thus attacking Automated teller machine networks is being a well organized and highly sophisticated way for cheating the bank clients.

![Figure. 3.1 virus attack in ATM computer](image)

The alternative, the attacker gains the complete control over Automated teller machine from distant location using a remote to control the Automated teller machine. To achieve gain remote access over Automated teller machine, the attacker must first exploit a vulnerability in the
Automated teller machines’ authorization process located in the remote control software, which happens to be ‘On’ by default for most Automated teller machines. Once attacker succeeds in establishing access over Automated teller machines’ through the remote management exploit, then he then updates command which allowed to install customized root kit. After Automated teller machines’ reboot, and with the root kit installed, the machine for its network settings and its physical location. Walking over to the compromised machine, and by inserting a custom credit card (or by entering a special key sequence), which grants access to the custom menu which is build by the attacker. From this menu, attacker is able to select any of the menu options available to him, and out came the money.

In another type vulnerability related to logical vulnerability of Automated teller machine, attacker empties one of the containers remotely – giving the unsuspecting passers by a Jackpot of their own. In this case, customized Automated teller machine control software could trace each and every ATM card that is inserted into the Automated teller machine; remotely downloading the log file and recording contained information of ATM card and saving it to storage device[50]. Later his information is used for unauthorized financial transaction.

Yet in another type Vulnerability is used against essentially a “weak point” in its programs or its concept, which could be used to overcome the security of the Automated teller machine. The Automated teller machine includes a set of hardware and software products (the devices, drivers, operating system, application programs, etc.) which operate in a pre-set manner following a chain of processes. The security of the Automated teller machine depends upon the security of the weakest link in the chain. In many cases, the operating system have weak link either due to its design or central control system of the Automated teller machine.

“STAND-IN” TIME
Automated teller machine behavior can change during “stand-in” time, where the bank’s cash dispensing network is unable to access databases that contain account information (possibly for database maintenance)[51]. In order to give customers access to cash, customers may be allowed to withdraw cash up to a certain amount that may be less than their usual daily withdrawal limit, but may still exceed the amount of available money in their accounts, which could result in fraud if the customers intentionally withdraw more money than what they had in their accounts.
C. COMMUNICATIONAL VULNERABILITY:

Mostly Automated teller machines are communicated with dial up lines or leased line to communicate with bank server. When a user process financial operation through Automated teller machine, machine verifies the authentication of user with ATM card data and send verification report to the server for financial transaction. If there is some vulnerability or weakness in network communication line exists hackers can easily tap the confidential financial information and use it in unauthorized operations. Attacker can implant new software (malware) in the network and gain control on Automated teller machine network and also gain control on bank server. This type of weakness is known as communicational vulnerability. There are so many causes which are generate the communicational vulnerability, few are discuss bellow:

STANDARD IT PROTOCOL USES WEAK ENCRYPTION

Financial data Communication in a network process in secure encrypted form. Some standard IT encryption protocols used in assessment systems were exploited due to encryption weaknesses. A published attack was used in multiple assessments to crack a terminal service encryption and view the user credentials during authentication. Remote desktop encryption can be cracked.

STANDARD IT PROTOCOL USES CLEAR TEXT AUTHENTICATION

Clear text authentication identification can be sniffed and used by an attacker to authenticate to the system. Here are two sanitized findings associated with this vulnerability from multiple assessments, Standard IT clear text authentication protocols are used by the control system in this Standard IT clear text authentication protocol services are running on multiple control system hosts. And hackers can easily tap the secure information these necessary services are vulnerable to attack, these services should be replaced with more secure counterparts. For example, the clear text protocols FTP, telnet, rshell, rexec, and rlogin can be replaced with SSH and secure FTP. This is straightforward for system access. This effort is not trivial if these services are integrated into the system functionality, and may require rewriting code, architecting secure authentication, or even reengineering system communications.
CONTROL SYSTEM PROTOCOL USES WEAK AUTHENTICATION

Commands from the Human-Machine Interface (HMI) cause actions in the control system. Alarms are sent to the HMI that notify operators of triggered events. The integrity and timely delivery of alarms and commands is critical in a control system. Weak authentication in control system protocols allows replay or spoof attacks to send unauthorized messages. This means it is possible to send messages that update the HMI or RTU. The attacker may be able to cause invalid data to be displayed on a console or create invalid commands or alarm messages[52].

The following specific assessment findings associated with this vulnerability were identified on multiple assessments:

Common control system protocol uses weak authentication between control system and field equipment (RTU)

Proprietary control system protocol uses weak authentication between control system components.

CONTROL SYSTEM PROTOCOL USES WEAK INTEGRITY CHECKS

The lack of, or weak, data integrity checks prevent a protocol from detecting bad data. An attacker is able to manipulate alarm or command messages sent over the wire if the control system protocol has poor integrity checks. This has the same effect as above, where the attacker may be able to cause invalid data to be displayed on a console or create invalid command or alarm messages. If an attacker has access to control system communication paths and reverse engineered the control system network communications protocol, it is possible to manipulate the data flowing between the system components. This includes commands and messages sent to update operator screens and control field equipment. Altering the operator’s view of the system received from the control system can be used to either trick the operator into performing actions the attacker wants, or to hide what an attacker is doing with the system.

Data integrity checks need to be designed and implemented in control system communication protocols. Use hardcoded Address Resolution Protocol (ARP) tables for static IP addresses or dynamic ARP inspection of dynamic IP addresses, if feasible. Monitoring the network traffic
for changing MAC addresses using an IDS, can help detect MITM attacks. Using port security on all network equipment is another good practice, which helps protect against unauthorized physical connections into the network.

**MITIGATIONS FOR VULNERABLE COMMUNICATIONS PROTOCOLS**

Control system vendors should implement secure-by-default settings for their control system products. These should include protocols that use strong encryption schemes for message authentication. Control system-specific protocols should be redesigned to include strong authentication and integrity checks. During control system configuration, vendors, owner/operators, and integrators should pay special attention to end-point security, including proper storage of encryption keys, signing of digital certificates, and enablement of security settings.

### 3.3 ATM CARDS

What is meant by the term “card technologies”? The simple answer is that any technology which uses a card for achieving the goal. To be specific what is a ATM card? Typical card coming in our mind our credit or bank card also known as banks plastic cards, these card are generally made of plastic viz polyester, pvc. Some time it is also made up of other material or even paper and it may or may not be amalgamation of materials. The main issue is that the ATM card has to be used to gain “access” over something. This technology includes some form or the form of automatic data collection and identification system i.e. of ADC/ID technology.

At present three main technologies are being used in technology for manufacturing ATM cards and the categories are (1) magnetic stripe cards, (2) smart cards and (3) optical cards. There are other technologies which are also in use in card technology and are being put to such bar codes having details of goods/commodity and touch memory, etc.. ATM card usually have printing on the cars and therefore it also involves other technologies viz Dye Diffusion Thermal Transfer, a technology required for printing the cards.

Functioning of optical and smart cards needs to illustrated to understand the technology in better way. More commonly used technology is magnetic stripe of card technology which has widespread use worldwide and gained popularity more viable solution for large numbers applications.
OPTICAL CARDS

The technology used Optical memory cards is similar to the technology used in manufacturing of music CDs also known as CD ROMs. A coat of the “gold colored”, which is a laser sensitive material have to be laminated on card. This coat has capacity to store the information. Coating material does comprise of single layer but is usually multi layers. These layers react once the laser light is directed to the Card. The laser is used to burns a tiny hole of approximately 2.25 microns in the coat layer and material is then has to be sensed by low power laser while reading the Card. The presence of the burn spot is indicated a “one” and or the absence of burn spot as a “zero”. The material on coat needs to be burned actually while writing i.e. the write cycle. The media used is suitable for write once read many known as WORM media. These data are non volatile meaning thereby that data cannot be lost if the power has been detached i.e. impression is permanent. The storage capacity of present day optical card vary between 4 and 6.6 MB of data. Optical cards are also capable to store graphical images viz fingerprints, pictures/photographs, logos, x-rays, etc.. The data on Optical cards are encoded in a linear format i.e. x-y format and confirms to ISO/IEC 11693 as well 11694 standards.

Optical technology in the present time has been widely accepted and is being used by Medical/ Healthcare industry; in Prepaid Debit Cards; for the Cargo Manifests; Seasonal Tickets, Admission Passes; for Maintenance of Auto records; and Retail Purchase Cards.

SMART CARDS

Smart cards are usually plastic cards of credit card-size but the card contains comparatively larger amounts of information imbedded into micro-chip. Smart cards has difference from magnetic stripe cards: (1) the amount of information which stored in smart card is much greater, (2) in place one time write memory smart cards do have capabilities to be reprogrammed such as to add or delete. Data on Smart card can be rearranged, in optical cards once written is permanent.

There are several terms which are being used for identifying cards having with embedded integrated circuits; the common terms are “chip card,” “integrated circuit card”, “smart card” but he cards known by all name really refer to one thing only. Smart card broadly divided in
two types. The first type also known as “dumb” card contains memory only and is used to simply store the information. Say one the dumb card has been embedded with value of one dollar, the said card will to store value cards as one dollar for example and holder of the card may spend the value i.e. one dollar in a variety of transactions such as to pay phone or for retail purchase or at any vending machines accepting the card with embedded inscriptions.

True “smart” card falls in second category. In true “smart card” a microprocessor has to be embedded in the card with memory. This card has capability in real sense to make decisions related to the data stored on these cards. These cards are not dependent on the unit to which the card has been plugged into for making application of any work, it is smart purse meaning a card for multi-use which is possible. The technology Smart cards give the choice to its user to have access on fairly large databases, which an user may require during travel be it an individual or an object. For example, smart card technology is being widely used to record the service histories of vehicle or automobile and the data travels with the automobile may be on a small tag which might had been placed in owner’s key ring. True “Smart cards” are reprogrammable and can be updated to have access all the service of vehicle on any outlet of the company’s dealers.

In order to provide a secure environment various methods are adopted to prevent access to the information on microprocessor card. These steps for the securities are being touted that smart cards has the capacity to replace other technologies.

Microprocessor type smart cards usually come in two versions – (1) the contact version, (2) contactless version. Both contact and contact less versions cards have microprocessor embedded. On the contactless version of microprocessor type smart cards one cannot notice of the gold plated contacts which are visible on the card. In contactless data is passed between the card and the reader without any physical contact having been made. The advantage the contactless system has since it do not require contact so wear out is reduced, electric shock for coming through the contacts is also avoided and so is the destroying the integrated circuit with the knowledge that the components are completely embedded in the plastic without any external connections. The disadvantage to contactless card is its limitations to the use.
Application for Smart card patent was filed as early as 1974 in France and but the first ever card was used dates back to 1982 also in France; so the smart card technology is not new by present day standards. The smart card technology was rapidly accepted in Europe when cost occurred on telecommunications verifications on-line was too high and smart card offered cheap transactions comparatively. The smart card too provides options, mechanism and opportunity for verification off line thus there is considerable reduction in the cost of transaction without sacrificing security. However in the United States, where the telecommunication cost is much lower compared to other countries specifically Europe, to gain momentum of smart cards use in United States had taken much longer time. Benefits of the acceptance of the smart card technology have depended for the purpose of its application as well as its real use. The Smart card has the ability to move large data at little cost. At present checks on vulnerability of the data i.e. to make the Smart card much more reliable for the use is under development.

A number of types of smart cards in use at present worldwide with growing demands. By 1993 number of smart cards produced by card manufacturers of repute stood approximately at 330 million. Share of true “smart cards” in 330 millions was mere 12% only. The bulk of the rest smart cards manufactured were cards with simple memory. Production of smart card by 1995 had gone up to approximately 580 million cards of which true smart card constituted about 10% share and the figure surged ahead to 990 million by 1996 but share of true card remained unchanged. Application wise from amongst card issued by 1993 approx. 260 million cards had reported to have put in use in communication systems and share in health sector applications stood at 25 million and another 23 million had reported to have been put in use by the banking sector. Small amount had also been reported to have put in use by various small projects and use in trials.

Future of the smart card is being looked at extremely bright and fast growing. Improvements and development taking place in the electronics industry worldwide had not left the smart card industry untouched but has resulted into increased capacities and ability of smart card. Manufacturing of integrated circuits or the state of the art used in technology has improved. At present it has become feasible to run smaller ICs on lower voltages and thereby lowering the power requirements but without any compromise on the capability of smart cards of holding more and more memory for processing. At present focus of development is toward increasing
the speed of smart card and it is likely to be addressed very soon. At present several seconds are consumed in only initialization of smart card and therefore single transaction may also take some time a longer duration which falls beyond tolerable limits for some transactions.

MAGNETIC STRIPE

The technology Magnetic stripe has gathered more momentum to make for use by common. Magnetic stripes have taken over a ride to become part of common men day to day life and have become inseparable. Magnetic stripes technology has been in use for past many years and new features are being added through development to improve it further and make it more compatible.

It was in early 1960’s when magnetic stripes on cards use was first reported. It was first deployed by London Transit Authority. A magnetic stripe system was installed by London Transit Authority in the London Underground. Bay Area Rapid Transit of USA, by the late 1960’s had also put in use a paper based ticket and the size of the paper ticket was of the same size as of the present credit cards. The technology used was based on storing value of the card on the magnetic stripe for reading. The stored value was rewritten with every use of the card was used by the user.

Though 1951 had seen first issue of Credit cards, but the card did not gain popularity for its use by common. It is the establishment of standards for the Credit Cards in 1970 that the magnetic stripe cards started gaining popularity and found its place in common use. At present standards’ of magnetic stripe cards is being regulated by ISO, which issue and amends the standards from time to time keeping in mind financial cards reliability for reading of the cards worldwide. At present transit cards of the magnetic stripe card constitute the largest share amongst all other users of magnetic stripe cards.

With the development of new technologies taking place, there had been predictions of the demise of the magnetic stripe but such prophecy has proved to be false with the investment in the current infrastructure it highly unlikely to be in near future. Magnetic stripe technology provides ideal solution to many facets and help in making our life easier. Magnetic stripe technology is inexpensive or at very cost and open for adoptions to numbers of functions. The
Analysis of Vulnerabilities in ATM Transactions

high coercivity of smart cards have been standardized for the financial institutions and such standardization has provided a fresh lease on life to smart cards industry. Advanced security features with latest techniques is available and it is expected that more development is expected on magnetic stripe technology in time to come.

WHAT IS A MAGNETIC STRIPE?

A magnetic stripe are strips of a black or brown stripe available at the back of a Card and one can visualize on ones credit card, or at the reverse side of airline ticket or other transit cards. The visible stripes contain tiny magnetic particles placed in a resin. tiny magnetic particles are either directly applied to the card. Sometimes tiny magnetic particles are shaped as stripe and placed on a plastic back by applying to the card.

The use of material for making of the particles imparts and controls the property of the Coercivity of the stripe. Particles of iron oxide are used as material for making of the Standard low Coercivity stripes. Particle of barium ferrite and other materials are used in manufacture of High Coercivity stripes. Particle of materials containing iron as mentioned above has to be added with a resin for formation of an uniform slurry. Slurry so prepared has to be coated onto a substrate. For manufacture of credit card or material for use in similar applications, the prepared slurry needs normally to be coated onto plastic sheet of good width and then dried. The coating of slurry is kept very very thin to avoid any obstructions in subsequent handling. The Sheet has to be sliced into stripes so as contain the stripes of iron particles is available on all card which was applied to the card in its manufacturing process. Other methods of application of iron particle are by lamination i.e. wherein the stripe and backing needs to be laminated into the card by hot-stamp. In such cases where heated die needs to be used for the transfer iron oxide stripe onto the card subsequent to card are cut to size. In case of the cold-peel, the oxide stripe is required to be peeled from back before the card is laminated. There are advantages and disadvantages of each method and way the stripes are manufactured and manufactures chooses the method for the intended end use of the product and user does not have a say except to choose types he or she wants.

One of the way for putting stripe on a card is that of direct coating of slurry containing iron particle. Usually iron oxide slurry are quoted in direct coating of the card, whether such card
are made up of paper or plastic. The direct coating method has the advantage of cost reductions in manufacturing of the cards but as far as quality is concerned there is compromise to certain extent.

Once the iron oxide slurry has been coated on the card either by the substrate method i.e. plastic backing or application of the particles directly to card stock, the iron particles present in the slurry has to be aligned. This arrangements of particles or aligning is required to have good signal compared to noise ratio. By this process pops and bangs are eliminated to larger extent. By pops and bangs refers to hearing on old tape recordings system. To align all iron particles on the card or tapes, the wet slurry has to be passed through a magnetic field. The use of iron oxide particles are for two reasons. The particles having low coercivity need smaller magnetic field for orientations. These particles are acicular i.e. they are needle shaped and have with aspect ratio of approximately six to one. The acicular particles have axis of magnetization along particles length. This axis magnetization makes process of the alignment to be easy. The high coercivity materials create difficulties in processing of the alignment of the axis of magnetization. The high coercivity materials particles does not possess acicular or needle shape. The materials mostly used for the high coercivity are be platelets. Platelets may have easy axis of magnetization. By the platelets, it is expressed that the alignment fields for axis of magnetization need to stand the particles on edge. If it can stand on edges, then only it can deliver the best performance out of the magnetic stripe. There is always likely hood that the particles shall fall over no sooner than the field is removed. Therefore great skill is needed in making of high quality stripe of high coercivity and needs skill during processing to keep those particles on required without any disturbance till the slurry has been set on the magnetic stripes.

The lack of alignment creates some major problems during the reading of the card during encoding the message available on the magnetic stripe. The wave shape acquired in high coercivity material affects the reading process of the card i.e. it creates some time distortions, which is result of the lack of alignment. Some time distortions are able to create significant errors and deny correct reading of the cards and there failure of desired activities.

After the above processes, the result is that the final card may have the familiar brown stripe or black stripe based colors of iron oxides and colors of resins. The stripes have capacities for
encoded only because it contains the particles of iron filings, which can get magnetized in the
directions of north or south pole only. It is change in the direction of the stripes which allows
encoding along length of stripes and thus the stripes are filled with required information to be
written on it. Information are required to be read back and modified if required if the magnetic
stripes had been encoded for the first time.

**WORKING OF THE MAGNETIC STRIPE:**

The end-use of the magnetic stripe calls for estimations of amount of data to be placed on
stripes as well as the signal amplitude expected on the stripes in order to meet the coercivity
requirement of the stripe and also that of encoding method as well the required bit density. The
card manufacturer select the material based on the first two points and after selecting of the
type of magnetic material for its use request the system designer to design on rest of parameters,
which are four.

As explained above, the magnetic stripes are product of many small particles which have been
bound together with resin. The controlling factors for the required signal amplitude are the
density of iron particles in resins. Higher is number of particles, it can generate signal of the
higher signal amplitude. The density of particle or loading combined with thickness stripes has
upper hand in controlling the amplitude. It is Signal amplitude which is matter of highest
importance, because Signal amplitude sets the limits for the designing of card-readers to read
the cards. Standards ISO/IEC 7811 have been set to regulate requirements of the signal amplitude
necessary for use in the requisite field say the banking sector. Cards are to be manufactured to
conform to the laid standards and its quality assurance is essentials for the magnetic stripe to be
read worldwide for unhindered financial transactions on Automated teller Machine terminal of
various models and make.

The bit density of the information has to be selected based on user requirement. The ISO/IEC
standards (7811) fix the requirements for the bit density for cards to be used in interchange
environment. The signal amplitude standards sets define tracks. The track one and three may
contains data of 210 bits per inch of its stripe. The track two may contain data up to 75 bits per
inch of magnetic stripe. It is the bit density in combination with the formats of data, which sets
limits of quantum of data which can be encoded on any track.
ENCODING OF INFORMATION ON THE MAGNETIC STRIPE:

Every character which is required to be encoded on a stripe do comprise of number of bits. The magnetic particles polarity in the stripes is needed to be modified for defining each bit. There are several systems which can be deployed for determining whether particular bit stands as a one or a zero. The system most commonly used for the purpose is F2F also known as Aiken BiPhase and MFM standing for Modified Frequency Modulation.

Standards ISO/IEC 7811 specifies the system for use in F2F encoding. Each bit is required to have the equal physical length on magnetic stripes in F2F encoding. The absence or presence of polarity change in centre of bit commands whether bit represents a one or a zero. The single bit width has always to remains constant. There are some bits which do have an extra polarity and its changes in the centre, such bit is called ones.

Modified Frequency Modulation encodings processes are more complex but have the advantages that since Modified Frequency Modulation encoding allows double amount of data to be encoded on same number of edges (flux reversals). Complete details of Modified Frequency Modulation are available with the AIM Inc have published it under title “Modified Frequency Modulation (MFM) for Magnetic Stripes”. Details can be taken from World Wide Web site of the AIM Inc.

The card manufacturers select the encoding scheme keeping in view the purpose to card shall be applied for the use, the end use of the cards. For example if intended application card does require conformance with ISO/IEC 7811 as an essential feature then F2F encoding should be the best choice. If the cards are intended for applications wherein large amounts of data are required to be encoded, Modified Frequency Modulation shall yield the best result. After the encodation scheme has been finalized looking to the purpose of the use of the card, thereafter the format of the data is also selected. ISO/IEC 7811 is having two different sets of the schemes for intended use on the cards. One of the scheme works on four bits plus parity for working. Other schemes work on six bits plus parity. In scheme of four bits, encoding of numbers are allowed with some control characters. But in scheme of six bits, the full alpha numeric set may easily be encoded. Parity bits have functions in determining the occurrences of an error, which would have taken place during reading of the data. The system works on basis where total
number of “one” bits in character are to be added up and in odd parity it must equal an odd number. If the total is odd, the parity bit is set to a zero, if the total is even the parity bit is set to a one.

ISO/IEC 7811 defines the encodation schemes. It is essential to follow directions of the scheme and then only applications shall conformance with 7811. Sometime the applications depart from the scheme and allows for different bit density/encoding scheme or combinations of schemes, others depart significantly by use of “proprietary” schemes down to the bit level. As an example, an identification card may use two bits to determine eye color (00 = blue, 01 = brown, 10 = green, 11 = other). These are much more efficient in encoding space, but means data cannot be read in a standard interchange terminal. For some applications it may not be important but the extra space available has high importance.

**COERCIVITY**

Magnetic stripes coercivity is measure in Oersteds (Oe). Oersteds is measurement system for the difficulties level of encoded information on a magnetic stripe. A bank card for general use usually have a coercivity level of approximately 300 Oersteds. This level of coercivity is classified as low coercivity. In Japan cards usually the card have double stripes or there are two magnetic stripes on single the credit cards level of coercivity of such card is 600 Oe. The present trend is use of magnetic stripes with much higher coercivity and values of coercivity of such cards may range from values of 2100, 2750, 3600 and 4000 Oersteds. Use of cards with high coercivity magnetic stripes has brought dimensions in manufacturing cards with new parameters but is misconceived factor that a magnetic stripe with higher coercivity shall always yield a better result..

Initial coercivity has to be defined by type of particles used for manufacturing the stripe. Whereas Gamma Ferric Oxide will give a low coercivity stripe, Barium Ferrite gives a high coercivity stripe. The material alone is not able to define the final coercivity of the stripe on the card as manufacturing process does change the values usually in the downwards direction and it is also possible to raise coercivity of particles by combining with other agents in the slurry. Coercivity is not a measurement of signal amplitude. In early versions of high coercivity stripes often used to have high signal output but it is not a requirement of high coercivity and high coercivity may
not always be a good thing. Most readers available now are setup to read signal levels equal to those defined in ISO/IEC 7811 standard. Keeping signal output in this range may make the range of available readers much greater.

In early versions of the high coercivity magnetic stripes were marketed in the name of High Energy; suggesting high output levels and often causing confusion amongst users for the technology.

**USE OF HIGH COERCIVITY**

The high coercivity has advantage that it is harder to encode information on the stripe and equally it is more difficult to erase information and thereby problems of accidental erase are also diminished. But still there exists the possibility to erase the information. Common household magnets may not be normally powerful enough. This means the person who has kept the transit card on the refrigerator by mistake, usually the encoding on the stripe shall not be damaged.

The disadvantages are that although the encoding can be read in a standard low coercivity reader the encoder must be designed to read encode of high coercivity stripes. Although the coercivity is factor in erasing the stripe, it is by no-means only factor. A stripe which has been declared to be a 4000 Oersted (Oe) stripe that actually means that the nominal value is 4000 Oe. There may be also lots of particles in that stripe with coercivities of other values. The distribution of the coercivities may typically follow a bell shape curve. The steepness of bell shape denotes the percentage of particles at stated value, a sharp (steep) curve shows that are large percentage are the nominal value. A flat curve indicates that there are many other coercivities present in the stripe. This is important because it is used to define something called “squareness” of the stripe. Squareness is a parameter which is used to help define the susceptibility of a stripe to erasure. A 2700 Oe magnetic stripe with high squareness (sharp curve) may have a large number of particles at the nominal coercivity. To erase that stripe, a magnetic force greater than the coercive value need to be applied to the stripe. Another stripe with low squareness does have a higher nominal coercivity but because there may be a large proportion of low coercivity particles it may be very easy to erase the stripe.
USES OF MAGNETIC STRIPE CARDS

Use of magnetic stripes is quite a common at present. The most visible use is banks’ credit, debit, and ATM cards, but these are not the only places where use of magnetic card user is limited. Airline Ticket and Boarding pass (ATB) also have magnetic strips. Many of these are now including magnetic stripes on the cards used as smart card used for metro tickets. Other use of magnetic cards used in phone card, transit i.e. bus or train ticket, and even parking lot ticket.

All the magnetic stripes are not all the same. From the outside it may look like same and seems to be all made of a magnetic material coated in some way on the document but by different ways of coating the material on the document and different ways of making the magnetic material they differ and these affect the performance of the material in many ways.

Manufacturing process regulates and controls properties of the magnetic stripe i.e. properties of cards are set during its manufacture. The properties which are regulated are signal strength of the encoding, coercivity of the magnetic stripes, capability of the card to withstand/resist erosions. Shape of the card for recording. These parameters has to be controlled by the user and have tremendous effect on the performance of the card and so has to be defined by the user.

Method of coating of cards with the magnetic material leaves its influence the card effecting the performance of the magnetic stripe of the card. A paper ticket, which is normally direct coating and stripe produced, is much prone to abrasions than the stripe which plastic card with lamination can bear to greater extents. Abrasiveness during the use of the card affects card life for its magnetic heads. Some manufactures of the card to protect the cards’ stripe from abrasion apply coating over magnetic stripes. Such coating over stripe to are applied to prolong the life of card or ticket for increased numbers of uses. Disadvantages of such coating is that such coating affect performance of stripe in number of ways.

STANDARDS FOR MAGNETIC STRIPE

The ISO/IEC 7810, 7811, 7812 and 7813 are the series of standards which are most commonly quoted standards at present use on magnetic stripes. These standards are being used by the
credit/debit card manufactures at present. In this system information as embossed characters are available on the cards and the track locations and the magnetic stripe. ISO/IEC 7811 standards is spread in six parts and parts two has tailor made standard for low coercivity magnetic stripes and part six of standard is specifically for high coercivity magnetic stripes. The standards set are for information (encoded) on the magnetic properties with guarantee that such strips are read unhindered by magnetic stripe reader world over. Along with standards of ISO/IEC 7811 series there are another standard known as ISO/IEC 10 373. ISO/IEC 7811 documents in details the testing methods for the series of standards laid down for magnetic stripes and forms under Regulations laid down by new American National Standards set to standardize the performance of magnetic stripe.

Three standards are:

- Effective Magnetic Parameters of Magnetic Stripes
- Suggested Magnetic Parameter Values for Applications
- Magnetic Stripe Readers and Encoders - Equipment Specifications

The new standards for are related to Effective Magnetic Parameters of Magnetic Stripes and Suggested Magnetic Parameter Values for Applications has been published by the AIM Inc. and are known as ANSI standard. Magnetic Stripe Readers and Encoders works on system that may be new in magnetic stripe technology with its aim to create standards which are relevant and useful for the equipment manufacturers.

Use of the cards is not limited to its use as debit card/credit cards for the use to carry banking transactions but these cards are use in other areas also in present day life. There are different sets of standards defining the track for reading viz the series of ISO/IEC 7811 allows to track one as a read and has 210 bits per inch and 6 bits plus a parity bit per character. This strength allows the full alpha as well as numeric encoding on the cards. Track two as well track three are in use at present and these are four bits plus a parity bit and can have number/characters plus A to F only with the difference that track two is compatible to 75 bits per inch as against track three is compatible to 210 bits per inch.
MAGNETIC STRIPE & SECURITY

Magnetic stripes are not fully secured. The process of manufacturing and encoding of Card has been simplified but this progress has made it easier for the crooks also to do the same. There are several schemes available which are being used to create a secure encoding on a magnetic stripe viz MagnePrint, Watermark Magnetics, XiShield, XSec, Holomagnetics, ValuGard, and Jitter Enhancement. All technologies have been added only to stop exploitations of some of aspects of the magnetic stripe used in Debit/credit card and attempt to ward stoppage of pilferages of the data available on the stripe of ATM cards but device to block the access has not been found feasible till date and poses difficulty ahead.

3.4 DEVICES MAKING ATMs VULNERABLE

CARD SKIMMER:

ATM card skimming has become common practice worldwide. The spread of the network of Automated teller machines as well as terminals at point of sale (POS) where merchandise is carried through acceptance of credit cards and debit cards having magnetic stripe for transacting the deals. At present highest number of ATM security issues and frauds through ATM are connected to stealing of information from ATM card or ATM skimming. Criminals are able to easily attach skimmer i.e. card skimming devices easily to card reader slot of Automated teller machines. Unprecedented growth of this evil device has been noticed and it is growing steadily with rise in numbers of Automated teller machines. Rise in menace of evils of ATM skimming fraud is matter of grave concern to all connected with industry and gained the significance. Card Skimmers are devices developed by criminals designed to capture information of the ATM card from its magnetic stripe. Usually Skimmers are designed to resemble with real slots of Automated teller machines’ card insertion slot and are mounted in such a way that user does not suspect that he or she has inserted or swiped his or her card through the fake dummy slot. The Skimmers are capable to copy and record information for manufacture of digital copy of the cards magnetic strip. With passing of time additional menace which has taken over is not limited only to copies the credit/debit card information, but also devices are capable to capture PIN numbers of the ATM Card.
Here few devices have been displayed bellow, these devices are commonly used for skimming. Skimming device is being installed onto card reader for getting the information of the card used by the user.

![Figure 3.2: skimmer device for installed at card reader slot](image)

The system of functioning of a Skimmer fixed in an Automated teller machine can be better understood by having an internal view of a skimmer. Picture of internal view of a Skimmer is placed herewith.

**View of internal of a Skimmer**

![Figure 3.3: ATM card reader skimmer internal view](image)
Whereas a custom-made skimmer kit displayed has been displayed, the internal view of skimmer is available at Figure 3.3. A Skimmer usually comprise of two components: An upper portion as displayed at Figure 3.2 comprise of molded device which can easily be mounted over card entry slot of Automated teller machine placed in a position so as to read the information of the ATM card’s magnetic stripe and record it for the use by the frauds.

![Figure 3.4 ATM card skimmer planted on modified atm component](image)

On many occasions comprised ATM card reader is attached magnetic stripe of card reader of Automated teller machine, as illustrated below:

![Figure 3.5 card acceptor slot overlay fixed to silicon-based magnetic stripe](image)

An illustration by picture of an actual card reader of Automated teller machine and side by side to an Automated teller machine fitted with over lay skimmer is given below:
The device illustrated at Figure 3.6 above is a card skimmer. The device has been fitted to the card acceptance slot of Automated teller machine manufactured under model No. Diebold Opteva 760, a machine which is very common in use and put into operation by manufacturers. The visible green circuit board in the picture is the device taken out of an MP3 music player[44].
A additional device in shape of card has been slide past the magnetic reader, visible as small black rectangle. The device can noticed to present at end of black and red wires near center in the picture. The MP3 component of music player listens the data during communication with the ATM cards, and device records the information as an audio file for storage into tiny embedded flash device having memory.

![Figure 3.8 skimmer keypad pasted on original keypad](image)

**Figure 3.8 skimmer keypad pasted on original keypad**

The device shown at Figure 3.8 is PIN capturing equipment and has been attached to the Automated teller machine as additional component. The device consists of dummy metal plate resembling to PIN entry pad and has been fixed in manner to rest just on top of the of PIN pad of the Automated teller machine in a fashion that when any key has been pressed it allows the PIN pad of Automated teller machine to record and to communicate Personal Identification number but prior signal is sent the real Automated teller machine, so that user can go through transactions, the device sends signal for recording to the fraudulent device[45].
PIN SPYING:

PIN spying devices are attached to normal working Automated teller machines, which records the PINs of ATM cards used by the clients on Automated teller machine and the same time, the frauds also do have access on PINs of ATM cards used for making illegal and unauthorized transactions.
PIN Spying using Spy camera: Fraud install in a fake advertising box or mailbox with small convert camera inside to observe PIN entry to an Automated teller machine in such a way that clients are not aware that communication made by users to Automated machine is being recorded by unscrupulous persons. With development of long life battery, the hidden camera can work for weeks together. Further advancements taking in wireless technology, unscrupulous persons is not required to come and physically collect the information captured by spy camera but the captured PIN are transited for use of data for producing counterfeit ATM card immediately[46].

PIN SPYING CAMERA BEING ATTACHED                 PIN SPYING CAMERA ATTACHED TO ATM

Figure 3.10 PIN spying camera

THE DROPLET METHOD

Small drops of oil are placed on the Automated teller machines’ keypad. After a customer has used the machine the thief can guess fairly and accurately which keys were pressed, the criminal will then go about stealing the ATM card used in the Automated teller machine. The banks recommends that customer must wipe the Keypad if the observe liquids on the keypad before the Automated teller machine is used for any transactions[47].

PIN INTERCEPTION

Some time sophisticated, battery operated and motion activated camera are placed in such a way in the vicinity of an Automated teller machine, so that it can record users entering their personal identification numbers at the Automated teller machine. The device, pictured below with the boxy housing in which it was discovered, was designed to fit into the corner of the
Automated teller machine framework and painted to match with Automated teller machine for the purpose of it is not noticed by the user.

![Figure. 3.11 self-contained camera and box](image1)

![Figure. 3.12 ATM front with and without spy camera](image2)
The Automated teller machine shown at Figure 3.12 on the right side is shown with installed the ATM card pin spying camera on top left hand side.

The “Camball-23 camera that was used for attacks, which retails for around $200 and runs for about 48 hours on motion detection mode.

The image below shows some of the manufacturer’s specs of The “Camball-23 camera which has capacity to run interrupted for days in row or 48 hours and has ability to detect motion of the surroundings.

![Figure. 3.13 camball-2 camera](image)

A closer look, it is relatively crude device attached to the mouth of the Auto teller machine card insert slot. It is designed to steal data recorded on the magnetic stripe on the back of all bank ATM cards. Criminals can encode the information onto counterfeit cards, and armed with the victim’s PIN, culprits withdraw money from the victim’s account from Automated teller machine around the world.

**CARD TRAPPING/FISHING**

Card trapping mechanism is made up some wire or other interrupting device attached to Automated teller machine card reader slot and traps the inserted card. As the ATM card of the user does not get ejected after use, the user thinks that there is some error in Automated teller machine and leave his ATM card inside the Automated teller machine. When user leave away from Automated teller machine housing, fraudster detach the cared trapping device and can access the ATM card.
Figure 3.14 card trapping and jamming device

Figure 3.14 shows the device attached to trapping the ATM card and device used for jamming the card by wire, or tapes or any other mechanism, which is inserted in the card entry slot.

THE LEBANESE LOOP

A discrete device is placed over the slot of Automated teller machine where customers insert their ATM cards. The machine then traps the card and a miniature camera placed at suitable details being fed by the user while communicating to Automated teller machine including PIN number being tapped on the keypad. The customer is unable to retrieve ATM cards and walks away, leaving the criminal to steal the ATM card. In a variation of this technique a skimming device is placed over the slot, which reads the details on the card’s magnetic strip. The data is later put on a mobile phone top up card’s magnetic strip – with the clone card then used like a regular ATM card at an Automated teller machine.

CASH TRAPPING USING DISPENSER FALSE FRONTS:

In this type of fraud attackers attached a false withdrawal shutter slot. The false withdrawal shutter slot causes cashes to get stuck inside when customers transact a withdrawal. The customer leaves Automated teller machine assuming that the Automated teller machine is out of order or goes to the bank to report the incident, in the mean time the thieves removes the false shutter slot to retrieve the notes and Cash trapped by false withdrawal shutter in the Automated teller machine.
SHOULDER SURFING

Shoulder surfing is method in which fraud stands closely to the person using the Automated teller machine and tries to observe the PIN being entered. An accomplice, who purposely kept out of view of the bank’s surveillance cameras, later mugs details of the victim of the ATM card. There are cases wherein it has been reported that binoculars are used by criminals from a nearby building to watch and note ATM card details including PIN of unsuspecting customers, while the customer uses Automated teller machine.

PARTIAL WITHDRAWALS

Similar to the Lebanese Loop where a thin sleeve is put to trap the ATM card, in this type of fraud cash is trapped by a sleeve or device slipped inside the cash dispenser. When a user operates the Automated teller machine, he feels the transactions of Automated teller machine is normally, but he does not receive full amount of transacted by him from the cash dispenser i.e. user receives partial amount. Remaining amount is stored in the false device attached to cash dispenser of Automated teller machine cash dispenser. As Automated teller machine is mechanical device, there is limit of communication with the Automated teller machine for a customer. Customer will either walk or drive away assuming the machine is out of order to lodge complaint. After customer has left, the thieves can walk in and remove the cash from the device.
RAM RAIDING

A ram raid is an attempt to remove an Automated teller machine and its contents, from its location, usually after battering through to the Automated teller machine with a motor vehicle. A ram raid involves an attempt to rip the Automated teller machine out of its position and remove it from its premises with the intention of breaking into the Automated teller machine to steal its cash. Ram raids take place when movement around the Automated teller machine is minimum i.e. dead of night or just after mid night when the intruders consider that there shall be no intervention of assumes to shall have to face minimum resistance from public and police[48]. This type of incident invariably causes considerable damage to the premises housing the Automated teller machine.

ROBBERIES / SAFE CUTTING VIA FRONTAL ATTACKS

The robbers subsequently break the wall of the Automated teller machine and decamp with the money inside. The robbers have cut the safe by cutter and steal money from it.

CARD MAGNETIC STRIP READER

Another type of vulnerability with ATM cards with magnetic strip, the strip is used in Automated teller machine without chip readers or when the chip is unreadable, leaving scope for the criminal to learn the contents of the magnetic stripe of ATM card and a cardholder’s PIN can withdraw cash by causing an Automated teller machine to fall back to the older system, or by using a copy of the ATM card in an Automated teller machine in a country such as the USA that has not adopted EMV. A copy of the magnetic stripe is stored on the chip in its public-key certificate and is sent to terminals (for backward-compatibility reasons), so PEDs must therefore protect not just PINs entered by cardholders but also other ATM card details. There may also be symmetric keys, used to protect communication between the PED and the bank, but these are outside the EMV protocol.

Merchants have free access to PEDs (as do corrupt employees), customers sometimes have access for long enough to tamper with them and fraudsters have impersonated service engineers to gain access. Thus the PED must be assumed to operate in an uncontrolled environment, and must also fulfill its protection goals subject to assumptions about attacker capabilities defined
in certification criteria. Currently the most economically important threat is that if the PIN and card details are intercepted when they are sent, unencrypted, between the card and PED, a fake magnetic strip card may be created.

3.5 SECURITY ANALYSIS AGAINST VULNERABILITIES:

The above given vulnerability information, security analysis is required and more straightforward for security strategy formulation. For each type of vulnerability one it is required to find all the boundaries it crosses, which provides a systematic way of working through the possibilities to establish whether those boundaries provide adequate protection. For each type, it is possible to see if the anti-tampering mechanism properly protects both data within it, and any enclosed tamper proof boundaries. This still does not make the analysis trivial, because it requires detailed work to establish which assets need to be protected against which vulnerability or a threats, and whether an individual security measure meets its requirements. However, this study steps permit experts in individual module design to establish the requirements for different types of security modules. This does not eliminate the need for system level analysis, but instead it assists the process of security building against above discussed vulnerabilities.

BIOMETRIC AUTHENTICATION IN THE CONTEXT OF ATMS:

While authentications of ATM card users on his bio-metric parameters still needs to be introduced in India, but it is use in some of the countries facing larger amounts of fraud through Automated teller machine. There were some experimental testing made scenarios in connection with Automated teller machines at the end of the 20th century (e.g. Dresdner Bank, Bank United of Texas). In recent years the banking organizations all over the world are desirous of implementing new “Chip card and PIN authentication schemes” in Automated teller machines in order to reduce ATM card fraud and costs of fraud. News have been published of security threats faced by about 40 Japanese banks, who have introduced biometric palm vein authentication technologies in about 19000 functional Automated teller machines. The vein is an externally invisible biometric feature and, therefore, difficult to copy. There are also projects in Brazil and in Austria related to introductions of biometric parameters for safe transactions at Automated teller machines. In Europe, the banking transaction of an automated teller machine is sent to the computer centre of the card issuing bank and there the customer authentication is performed.
centrally on main frame computers/servers. Therefore, in this case, it is essential that banks maintain biometric templates in a central database of its customers and it is recommended to keep such data protected and inaccessible from alteration or modification to prevent fraud. Especially, the method of protecting biometric templates by error-correcting and cryptographic methods could be practiced, as described in the following text.

The values of false acceptance rate by Automated teller machine in vein based biometric solutions, as published by banks are 0.00008% and 0.0001%. Therefore, even for vein based biometrics the problem will remain there and not solved, yet. It is advisable to combine the biometric method with the traditional PIN and chip schemes, “This mechanism ensures a three stage security solution; ensuring users provide something they ‘own’ (the card), something they ‘know’ (the pin) and something they ‘are’ (the biometric identifier) before the transaction is processed”.

Another major challenge for the future will be to create new international standards for personal identification schemes including biometric authentication technologies in order to guarantee interoperability between different banking organizations and countries. One approach is the generalization of the existing international banking standards, and combining them with the biometric template protection approach.

The banking industry actually supports many different PIN generation and verifying procedures and formats. For the VISA PVV PIN Algorithm, which supports a non-secret PIN Verification Value (PVV), here suggested a generalization of the PIN procedure in the following way, introducing biometric technologies. The major aim for this generalization is to allow the introduction of biometric technology with minimal changes in the actual standards and hardware implementations. According to the scheme of Jules and Wattenberg, in a banking card personalization centre, a random codeword, i.e. \( c = G(s) \) for a random \( s \in \text{GF}(q)^k \), is bitwise added (XOR) to the biometric template \( f \) of the cardholder during enrolment and the result is stored on the banking card as \( y = c \oplus f \). Then the secret value \( s \) is hashed with a cryptographic hash function to obtain \( H(s) \). After generating a secret PIN, the hash value \( H(s) \) is used as a new input parameter to produce the non-secret PIN verification value PVV in a generalized way, combining conventional PIN procedures and biometric technologies. The biometric data is introduced as one non-secret parameter, the parameter
“data_array-Reserved-2” and “data array-Reserved-3” of the API “Clear PIN Generate Alternative” could be used for this purpose [37]. If a customer uses an automated teller machine, he enters his secret PIN. Furthermore, a biometric feature is extracted and a biometric template is generated. In the banking card this biometric template \( f^* \), presented by the user, is added to the value \( y \) stored in the banking card. The result is \( f^* \oplus y = f^* \oplus c \oplus f \). Since we are working with an error correcting code, the corresponding decode function produces a value \( s^* \). If the hamming distance between \( f^* \) and \( f \) is at most \( t \), then \( s^* = s \), otherwise not. After hashing the received value \( s^* \), \( H(s^*) \) is integrated into the banking transaction together with the encrypted PIN. The banking transaction is encrypted and sent to the banking authorization centre. In the banking authorization centre the transaction is decrypted [38].

The encrypted PIN and the hash value \( H(s^*) \) are extracted together with other parameters, the PVV, the account number, and are used as input parameters for the PIN verification procedure. The generalized PIN verification procedure generates a new PVV-value \( PVV^* \), corresponding to the supplied PIN, account information, hash value \( H(s^*) \) and other parameters and compares it with the input-PVV. If the \( PVV^* = PVV \), the user is authenticated. If an authorization fails, the retry counter can be limited by a small value in order to prevent brute force attacks.