Banking and Bookkeeping

Chapter 10 :

Ross Andresson's book "Security Engineering"

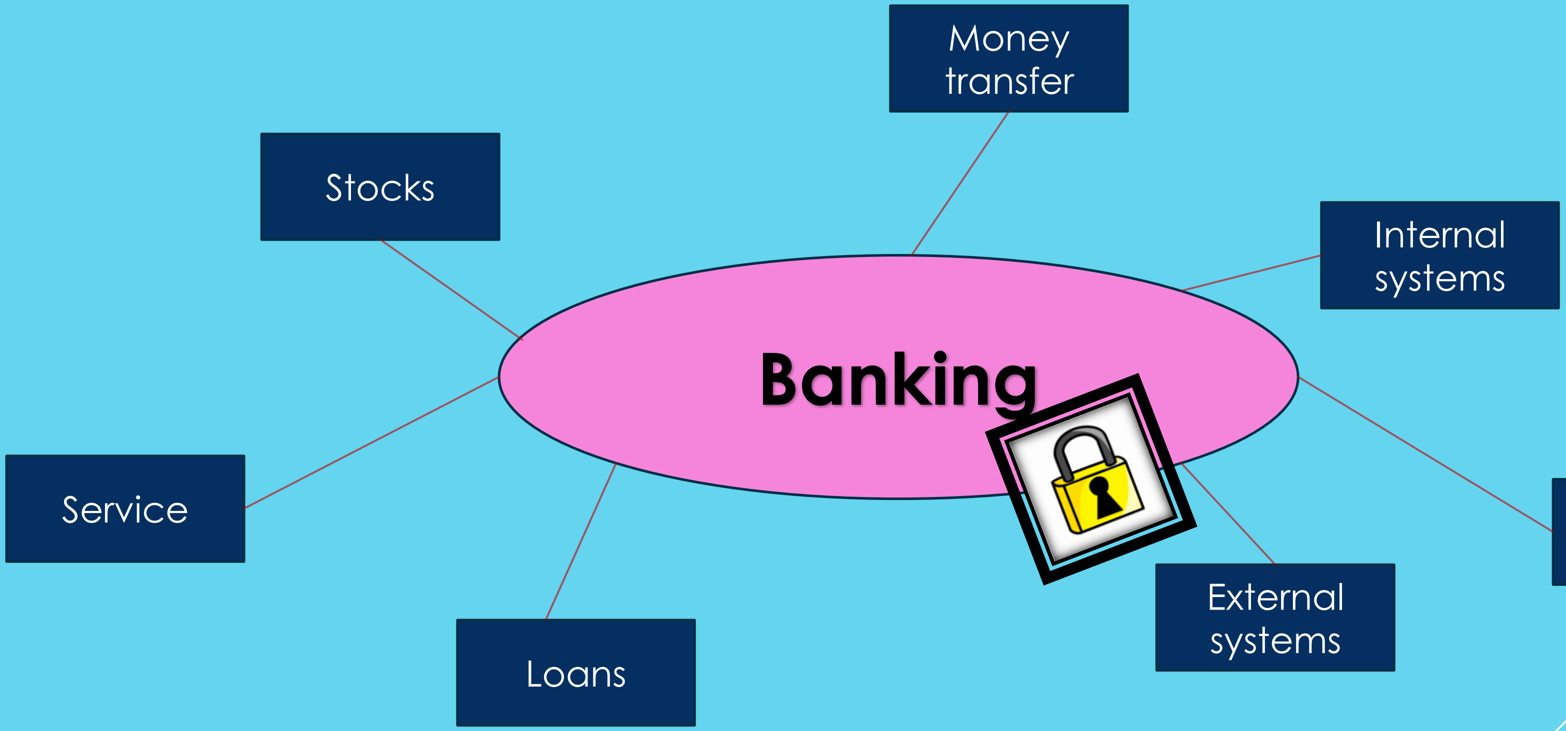
Security Seminar 2016

Presented By : Lior Portnoy

Outline

- Introduction
- Banking and Bookkeeping
- SWIFT
- ATM
- Credit Cards
- Smart Cards
- Summary

Introduction



Banking

Money transfer

Stocks

Internal systems

Service

Bank accounts

External systems

Loans

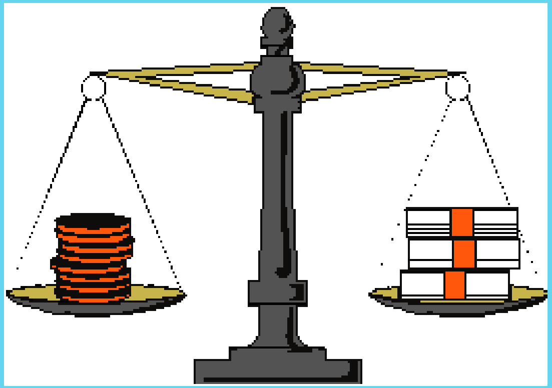
Banking and Bookkeeping

Double-Entry

► The idea – each transaction is posted to two separate books.

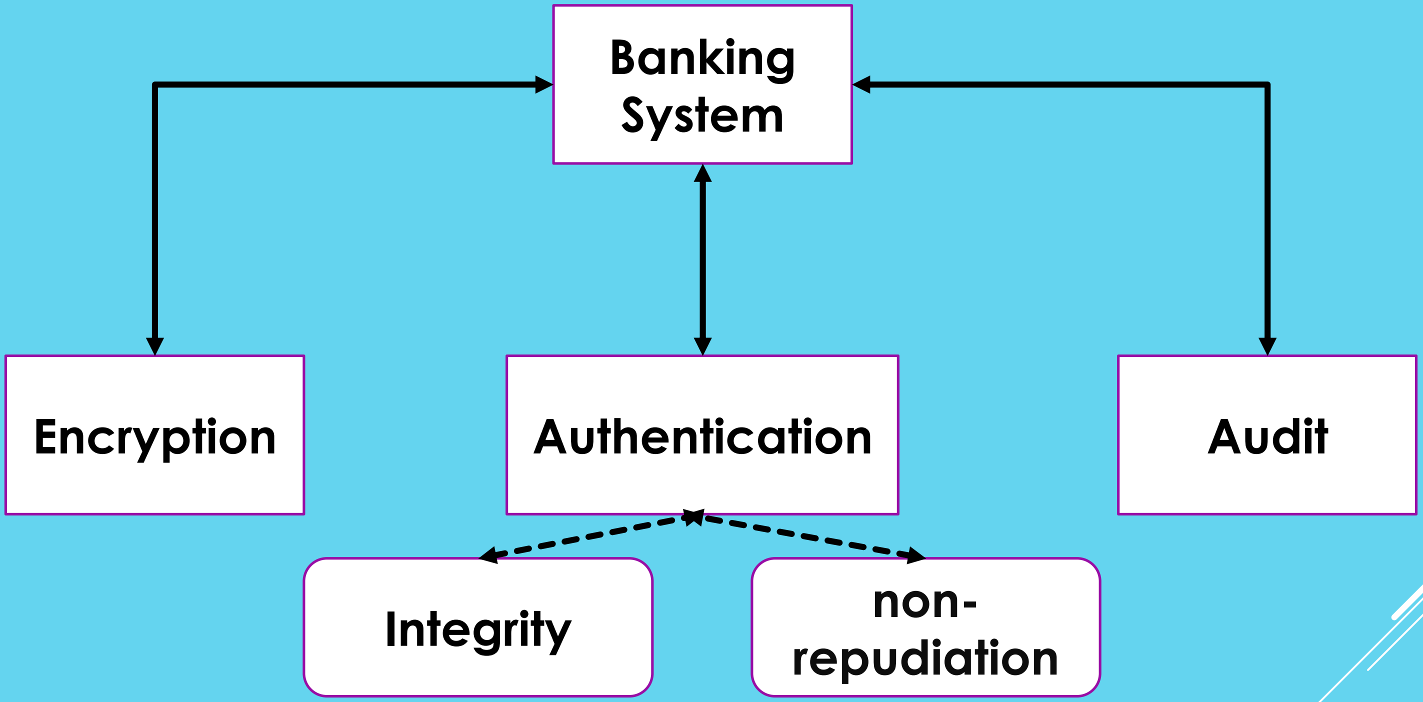
► At the end of the day, the books should balance.
the assets and the liabilities should be equal.

► Most frauds need the collusion of two or more members.



Banking and Bookkeeping

Basic



Banking System

Encryption

Authentication

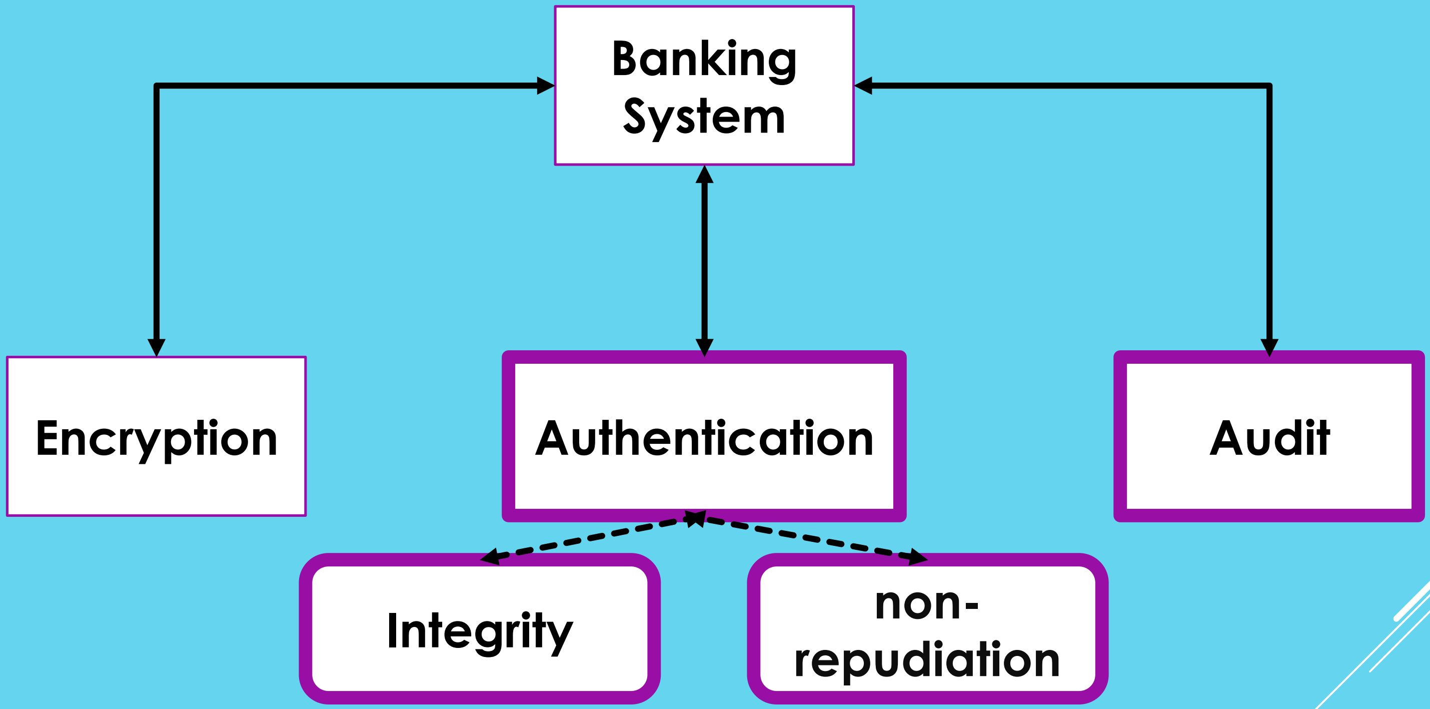
Audit

Integrity

non-repudiation

Banking and Bookkeeping

Basic


Banking System

Encryption

Authentication

Audit

Integrity

non-repudiation

Banking and Bookkeeping

► The banks are using computers for bookkeeping.

► Need to record & supervise every operation and transaction.

► Security – as technology evolved need to make more efforts to secure the system – in\out treats.

► Example for security policy model …. (Focus on <u>integrity</u>)

Banking and Bookkeeping (2)

The Clark-Wilson Security Policy Model

1. The system will have an ***IVP*** for validating the integrity of any ***CDI***;
2. The application of a ***TP*** to any ***CDI*** must maintain its integrity;
3. A ***CDI*** can only be changed by a ***TP***;
4. Subjects can only initiate certain ***TPs*** on certain ***CDIs***;
5. Triples must enforce an appropriate separation-of-duty policy on subjects;
6. Certain special ***TPs*** on ***UDIs*** can procedure ***CDIs*** as output;
7. Each application of a ***TP*** must cause enough information to reconstruct it to be written to a special append-only ***CDI***;
8. The system must authenticate subjects attempting to initiate a ***TP***;
9. The system must let only special subjects (i.e. security officers) make changes to authorization-related lists;

UDI – unconstrained data item. CDI – constrained data item.
IVP – integrity verification procedures. TP – transformation procedures.

Banking and Bookkeeping (2)

The Clark-Wilson Security Policy Model

1. The system will have an ***IVP*** for validating the integrity of any ***CDI***;

3. A ***CDI*** can only be changed by a ***TP***;

6. Certain special ***TPs*** on ***UDIs*** can procedure ***CDIs*** as output;

8. The system must authenticate subjects attempting to initiate a ***TP***;

UDI – unconstrained data item. CDI – constrained data item.
IVP – integrity verification procedures. TP – transformation procedures.

SWIFT

Background

► As the financial system evolved, created a need to define and implement “common language” to communicate and perform transactions.
For example – requirements :

** currency conversion .
** Sync payments worldwide.
** secure – encryption, authentication, non-repudiation services.
** save logs about transactions.

► SWIFT was set up in the 1970s by consortium of banks.
at start in Europe and after it spread to banks all over the world.

SWIFT

Society for **W**orldwide **I**nterbank
Financial **T**elecommunication

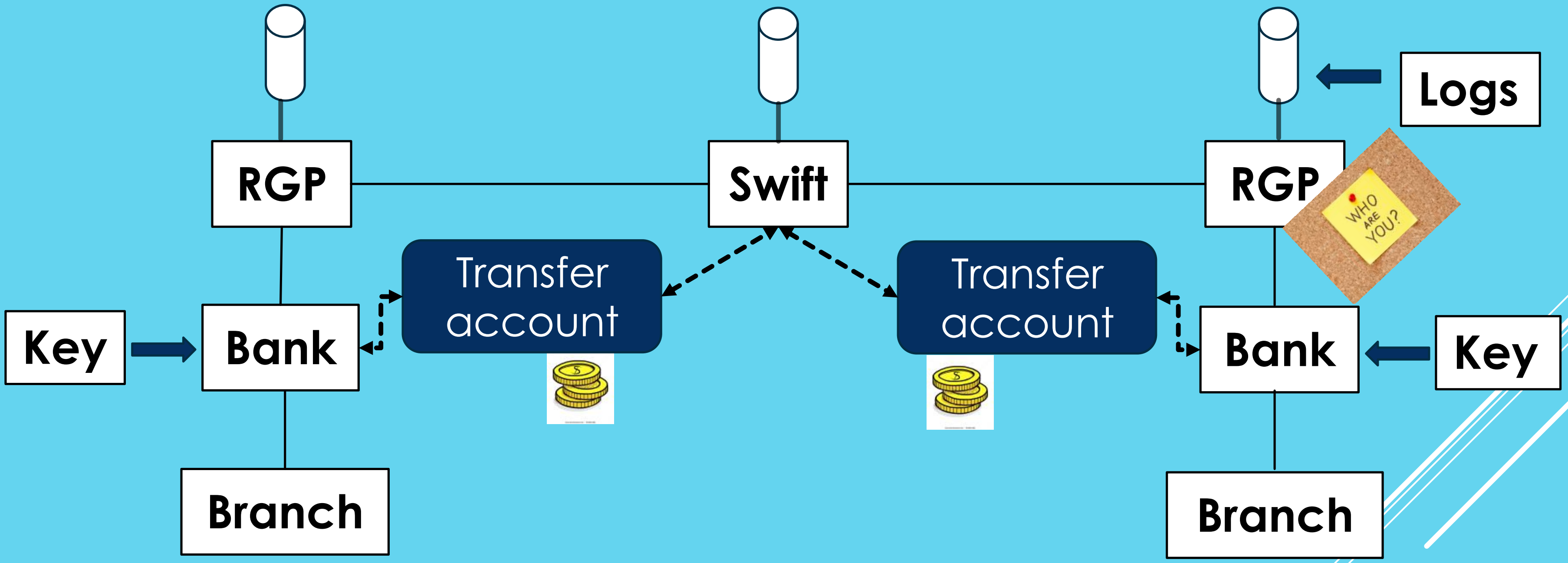
► **The *Society for Worldwide Interbank Financial Telecommunication (SWIFT)* provides a network that enables financial institutions worldwide to send and receive information about financial transactions in a secure, standardized and reliable environment. ***

► **First we will discuss system architecture and than what go wrong throw years.**

--- -
-
* Wikipedia

SWIFT

Architecture



RGP

Swift

RGP

Logs

Transfer account

Transfer account

Key

Bank

Bank

Key

Branch

Branch

SWIFT
Architecture (2)

- **System with built-in encryption, authentication and non-repudiation.**

- **The banks do not trust SWIFT thus the banks that want to connect with each other need to agree on key for authentication and encryption.**

- **Non-repudiation is achieved by using RGP (*Regional General Processor*)that used as mediator between the banks and SWIFT system. used especially when banks has world wide activity.**

- **Another way to see RGP is to think about PKI (issue from security).**

SWIFT
What Goes Wrong ?

► Almost not knowing about external fraud in SWIFT system because banks are using public key mechanisms for sharing key for authentication and encryption.

► Most of the attacks are internal :

-> Internal software in bank with bug.

-> Trojan software in banks computer’s.

all the attacks lead to false transactions between the banks (with purpose or without).

► Another attack is by using fake SWIFT message for authenticate order between two banks.

ATM
Automatic Teller Machine

► An ATM is an electronic device which allows a bank’s customer to make cash withdrawals and check their account balance at any time without the need for a human teller.

► Many ATMs also allow to deposit cash or cheques and to transfer money between their bank accounts.

ATM
Basics

► Every customer that use the ATM need to use magnetic card.

► The magnetic card contain customer account information and encrypted data according to the customer PIN number.

► Early ATMs also operated offline thus it contain with all customers data – very complicated for design and to secure.

► In recent years networks have becomes more dependable and ATMs operate online (simple design for ATMs and magnetic cards).

ATM
Basics (2)

► Two ways to implement ATM security hardware and software.

► A cryptographic processor (security module), is kept in the bank's server room and perform operations on PINs and related keys to enforce dual-control policy.
This includes the following :

- ► ► Operations on the clear values of customer PINs – no member of bank's staff can see the clear values.
- ► ► The card and the PIN is sent to the customer by separate channels.
- ► ► A terminal master key is supplied to each ATM by two separate officials.
- ► ► Create PIN number encrypted by terminal master key if ATM need to perform verification locally.
- ► ► If the PIN verification need to be done in central place – check the encrypted PIN number
- ► ► PIN translation when ATM accept other banks customers.

ATM
Basics (3)

► ATM network has major increase throw years.

► Many banks used software encryption rather than hardware Security.

** The programmers have access to PINs customers information.

** More hard to standardized.

► The ability to handle with frauds is more efficient when using hardware security.

ATM
What Goes Wrong ?

► Even when the technology evolved still throw years many fraud discovered in ATM network.

► The engineers who designed ATM security had assumed that criminals would be relatively sophisticated … ☹ but the trues is that there are many frauds that made by people with no knowledge about the system design.

► Attack ‘Surfing shoulder’ – attacker stand in line behind a victim, and see what PIN number he entered and pick up the discarded ATM slip.

ATM

What Goes Wrong ? (2)

- Attack ‘Copying card’ – attacker install on ATM gadget that normal user do not pay attention to it and than when the user insert his card to the ATM it copying the data.

- Attack ‘False terminal’ – attacker set fake ATM terminal and collect information about customers.

- Attack ‘Steal the ATM’ – attackers still the ATM machine.

https://www.youtube.com/watch?v=E9tl4t79Yvc

Credit Cards

► The main financial tool today for trading.

► It can be used for classic trading and on-line trading.

► The on-line trading exposed the banks and the card's companies to challenging security issues.

► In the last years the chip technology entered to the credit card world – it add more security.

► Every transaction of payment in credit card throw one or more companies make income to the companies and make the growing use of credit cards worthy.

Credit Cards

Fraud

► In fraud we distinguish between two main issues :
** Real use – Actual using lost\stolen card.
** On-Line use – Using someone else card to order goods in internet or other type of communication that not need to present in the ordering process.

► Now days every operation in card can be verified with the credit company on-line.

► Not all the time it is important to verify the ordering via the credit company even if the falling cost of communications.
In specific times the credit companies take the risk of fraud or forgery – Risk Assessment .

Credit Cards

Fraud (2)

- Banks manage the risk by using expiry date, lowering the floor limit, increase commission, insisting on delivery to the card older address and etc. .

- Sometimes for add more security when ordering on-line the system ask from the customer to answer a question.
  but this is, again, can open option for phishing attack …
  “What is your PIN number ?”

Credit Cards

Forgery

► As in ATM part, crooks can duplicate the cards with the magnetic data.

► It's a 'Cat and Mouse Play' for every challenge that the banks and credit companies add to secure orders,
the crooks response and override it.

► Now lets summarize some challenges that used for secure ->

** Terminal draft capture – where a sales draft is printed automatically using the data on the card strip.

** CCV card verification values – three digit that are output of MACs computed on the card strip content.

** Using chip technology on the credit card.

Credit Cards

Forgery (2)

► Now lets summarize some crooks response to above challenges :

** Flood of forged cards.

** Skimming – swipe cards using an extra, unauthorized, terminal to grab a copy of the magnetic strip, which would be re-encoded on a genuine card.

** Crooked businesses which skim card data and absorb the cost of customer transaction.

** Ability to duplicate smart cards with chip (Not so simple).

Credit Cards

Automatic Fraud Detection

► You don't need a gun to rob a bank any more. Now a bank robber's most powerful weapon is a computer and an internet connection.

► To reduce the risks, banks themselves are using more sophisticated technologies.

** On-line monitoring of accounts and credit cards transactions using database of information that about every account history.

** Off-line analysis of accounts and credit cards transactions.

** Banks and credit companies are analyzing the employs operations on-line and off-line.

Credit Cards
The Economics of Fraud

► As on-line commerce evolved fast the banks and the credit companies have great interest to secure it but not all the time – risk assessment.

► In the last years the loss from on-line commerce via credit cards frauds become less percentage.

► The success of lowering the percentage of loss in frauds is because of two main reasons :

1. As we speak before, the banks and companies using variety of secure technologies.
2. The regulators in states force by lows the banks and companies to secure the system.

Smartcard-Based Banking

► Smart cards are bank cards with chip inside it.

► The chip contain capability to verify a PIN and authenticate a transaction.

► The outcome of the chip is encrypted data that depend on PIN number and the account data in the magnetic strip and the current purchase information.

► This technology not implemented in all states.

► As this technology become widely and the demand for secure, the need for standard for using cards with chip became more necessary.

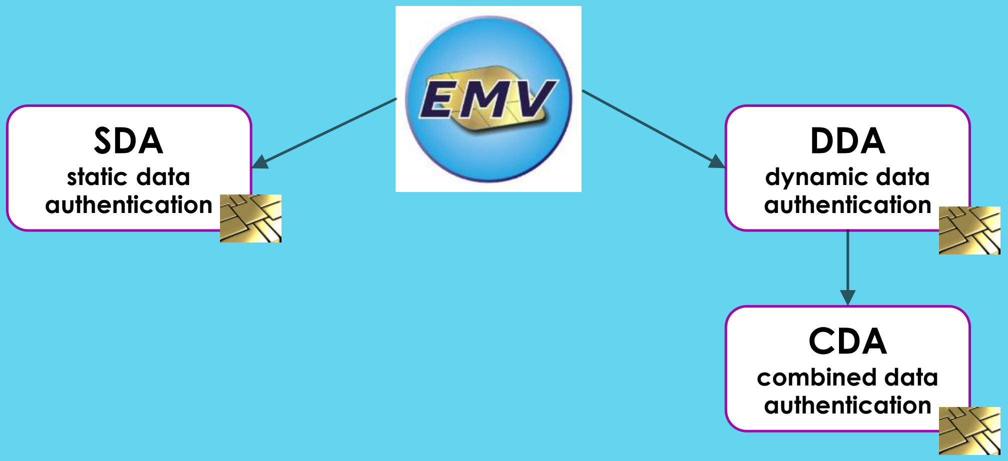
Smartcard-Based Banking

EMV

- The EMV standards are name after ‘Europay,Mastercard,VISA’.

- Technical standard for smart payment cards and for payment terminals and automated teller machines that can accept them.

- The cards come in two types :



SDA
static data authentication

DDA
dynamic data authentication

CDA
combined data authentication

Smartcard-Based Banking
EMV - SDA

► The customer puts her card into the ‘chip and PIN’ terminal that sign strip data.

► The terminal verify the signature and the merchant enters the payment amount.

► The customer asked to enter PIN number.

►If all approved the card create MAC for signature the data between user and the bank.

Smartcard-Based Banking
EMV – SDA (2)

► The protocol has a number of vulnerabilities :

** ‘Backwards compatibility’ – with magnetic strip cards, the information that signature contain all the data in the strip line. now crooks can sniff to data and duplicate the card without even knowing the PIN number.

** If the card reader and PIN pad are separated – crooks can listen to data in air.

** Spy chip devices – under the terminals.

** Authentication methods – each card and terminal, has list of procedures ‘on-line PIN’, ‘local PIN verification’, ‘no authenticate’ -> it option that the last procedure will run (problem with authentication).

Smartcard-Based Banking

EMV – DDA

► More complex EMV protocol.

► It differs from SDA in that the cards are capable of doing public-key cryptography -> each has an RSA public-private key pair.

► This provides a small amount of extra protection – the PIN doesn't travel in the clear between the PIN pad and the terminal.

► The protocol has a number of vulnerabilities :

** If there is hard link between the public-key operation of proving freshness and accepting the PIN, and MAC (authentication methods).

** No protect when someone can analyze what PIN entered in the terminal keypad.

Smartcard-Based Banking
EMV – CDA

► This protocol is improve of DDA. it’s like DDA except that the card also computes a signature on the MAC.

► The protocol has a number of vulnerabilities :

** Even if the protocol is more secure there is problem that the customer has no trustworthy user interface.

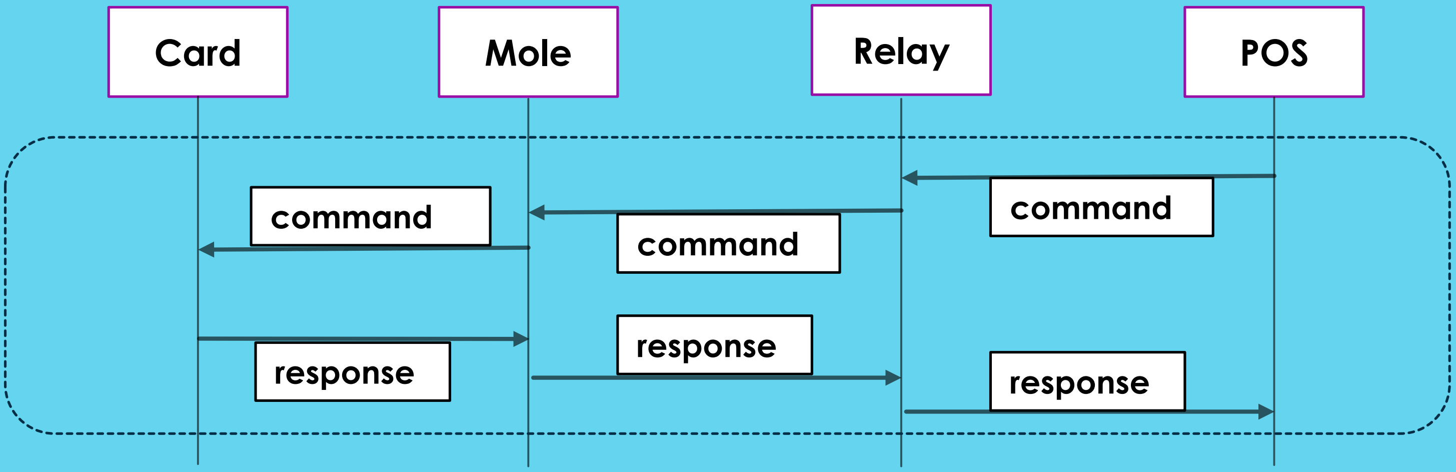
** ’Social engineering’ attacks – observe PIN entered, bogus vending machine …

** Relay attack -> (+ replay attack)

Smartcard-Based Banking

EMV – CDA (2)

► With a relay setup, the POS terminal is tricked in thinking it is acting directly with a card, while the card is tricked in thinking it is acting directly with a POS terminal. In reality, both card and terminal each act with a different device. *



-

* http://www.cs.bham.ac.uk/~tpc/Relay/thesisJordi.pdf

Smartcard-Based Banking

RFID

- ► Contactless payment cards.

- ► The card contain RF device that communicate with terminal.

- ► The protocol has a number of vulnerabilities :

** The card can be use as regular card with all traditional attacks.

** The attacker can get card data contactless.

** ‘Man In The Middle’ – attack.

** When you hold more than one card – what card to charge?

Summary

► We described in this presentation various of financial tools for using and maintain bookkeeping in banks.

► The secure of those operations is necessary as the using of the tools is increase – with emphasis on authentication and audit.

► When we come to design security model for system we need to also pay attention for “simple” attackers that not necessarily know the how break encryption or authentication data.

► As customers we have an opportunity to reinforce the ‘Audit’ part of the system.

ATM SECURITY

Thank You ! ☺