Banking and Bookkeeping

Ross Andresson's

book "Security Engineering"

Presented By : Igal Rabaev

https://www.123rf.com/

Lecture Questions we will answer

- Can we trust banks?
- Can we trust its employees?
- Can we trust merchants?
- How should we behave as costumers?
- What should the bank change?
- What should the government do?

A bit of history

Figure 10.1: Clay envelope and its content of tokens representing 7 jars of oil, from Uruk, present day Iraq, ca. 3300 BC (Courtesy Denise Schmandt-Besserat and the Louvre Museum)

- Bookkeeping started 8500 BC, when people started producing surplus food, which led to storing and trading.
- Food represented by a clay token, which was placed inside a clay envelope and sealed by rolling it with the pattern of the warehouse keeper.
- Later they started to make the tokens from metal, and after, they stamped the tokens themselves, thus invented the coins.

A bit of history

- As trade grew, businesses became too large for a single family to manage, so they opened branches. Which led hiring workers.
- This has led to **double-entry bookkeeping**

Double-Entry Bookkeeping

- Each transaction is posted to two separate books, as a credit in one and a debit in the other. In the end of the day, the books must balance.
- Both books can't be held by the same person. Forces **Dual-Control.**

https://tenor.com/view/perfectly-balanced-thanos-infinity-war-gif-13078930

Types of Frauds

Inside Frauds – Banks

Outside Frauds – ATM, Credit Cards

Types of Frauds

Inside Frauds – Banks

Outside Frauds – ATM, Credit Cards

Bank Computer Systems

- Banks were among the first to use computers for bookkeeping.
  - Check processing, payroll services, ATM's…
- Implemented the double entry principal.
- Data Structures:
  - Account master file: tracks a costumer balance and transactions for 90 days.
  - Ledgers: tracks cash and assets
  - Journals: hold transactions outside the bank: ATM…
  - Audit trial: tracks which worker did what

Designing an internal control system

- Two or more different staff members act on a transaction at different points in its path.
- Model can be described as *prevent —detect — recover (the frauds.)*.
- It is essential to put extra effort into prevention, using techniques such as dual control.
- Where prevention is hard, you should see to it that detection is fast enough, and recovery vigorous enough, to provide a deterrent effect

Designing an internal control system difficulties

- Highly interdisciplinary problem.
- Human factors are very often neglected.
- Workers ignore protocols, laziness.

Designing an internal control system Main Issue

Indeed, at banks I've helped with security, you will find that there are thirty or forty people whom you just have to trust— the CEO, the chief dealer, the top sysadmins and a number of others.

The Clark-Wilson Security Policy Model

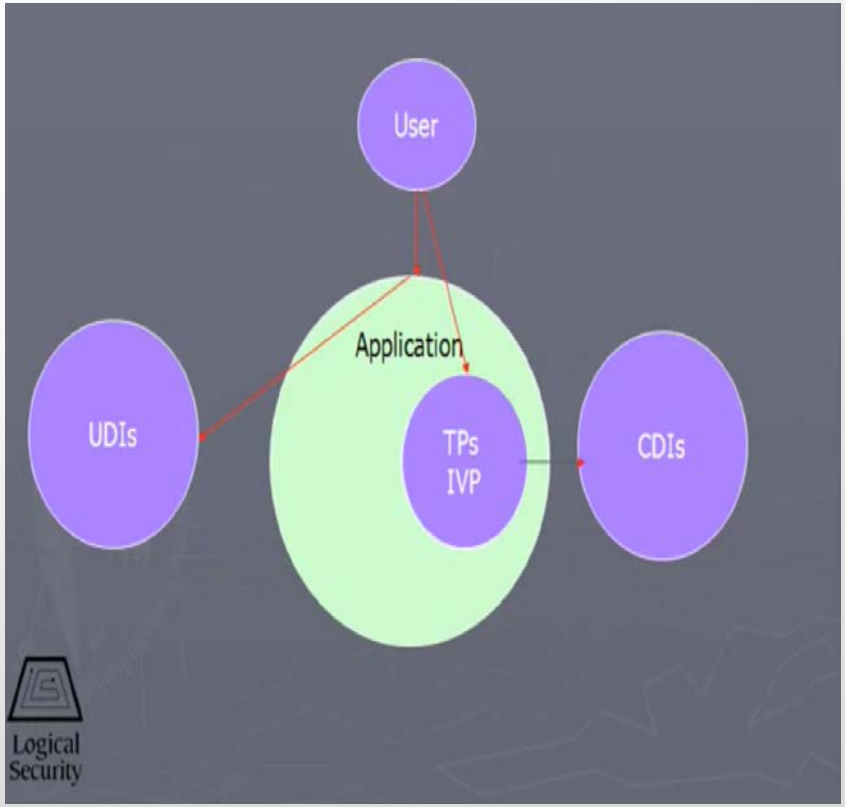
1. The system will have an IVP for validating the integrity of any CDI.

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.



https://www.youtube.com/watch?v=Wd3454UQ4kw

The Clark-Wilson Security Policy Model

6. Certain special TPs on UDIs can produce 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.

Bucks Co. bank manager headed to prison for theft

Source: https://www.wmur.com/article/former-portsmouth-bank-manager-indicted-on-theft-charges/26001828

Source: https://6abc.com/bucks-co-bank-manager-headed-to-prison-for-theft/2432706/

Former Oakhurst bank manager charged with grand theft

by FOX26 NEWS | Friday, May 18th 2018

Source: https://kmph.com/news/local/former-oakhurst-bank-manager-charged-with-grand-theft

Bank - What goes wrong

- reports that 82% of the worst frauds were committed by employees.
- nearly half of the perpetrators had been there over five years and a third of them were managers.
- Examples:
  - A Bank did not audit address changes, so a worker changed a costumer's address and ordered a new credit card, then changed it right back.
  - Paul Stubbs, a password reset clerk at HSBC
  - The murder of Mala Milevski
  - The Trading bank embezzlement (Eti Alon)

SWIFT transfers between banks

- Then SWIFT-Society for Worldwide International Financial Telecommunications
- Physical key exchange between banks.
- The usual method of operation is to have three separate staff to do a SWIFT transaction: one to enter it, one to check it, and one to authorize it.(triple control)

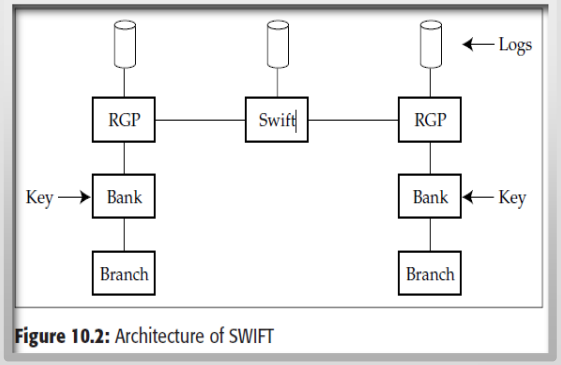


Figure 10.2: Architecture of SWIFT

SWIFT
What Goes Wrong

- Most tries were of programmers who didn't fully understood the system, so they got arrested quickly.
- Example: Bank manager in Johannesburg abused rates.

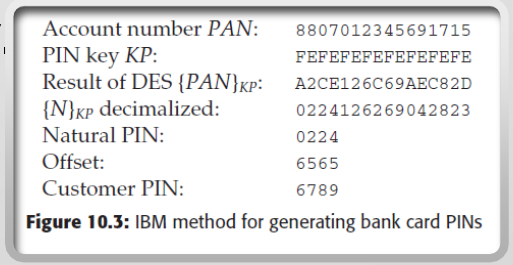
Types of Frauds

Inside Frauds – Banks

Outside Frauds – ATM, Credit Cards

ATM
Automatic Teller Machines

- Used to withdraw cash.
- In order to withdraw cash you need a magnetic card .
- The card contains the customer's primary account number, *PAN*.
- A secret key, called the 'PIN key', is used to encrypt the account number, to decimalize it and truncate it.
- In the first ATMs to use PINs, each ATM contained a copy of the PIN key and each card contained the offset as well as the primary account number.
- In recent years networks have become more dependable and ATMs have tended to operate online only.

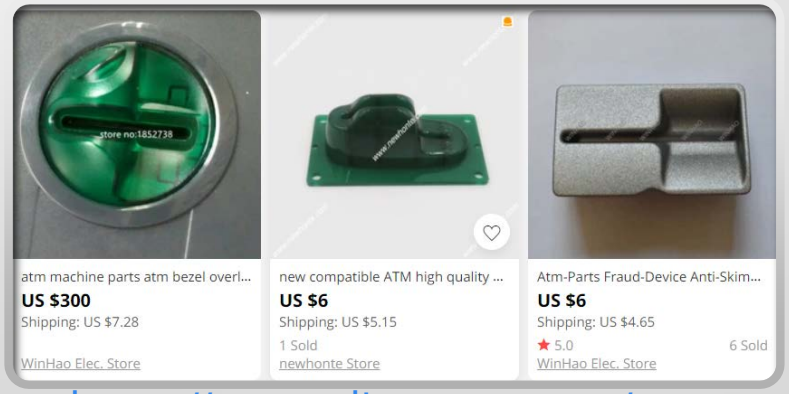


Account number *PAN*:	8807012345691715
PIN key *KP*:	FEFEFEFEFEFEFEFE
Result of DES $\{PAN\}_{KP}$:	A2CE126C69AEC82D
$\{N\}_{KP}$ decimalized:	0224126269042823
Natural PIN:	0224
Offset:	6565
Customer PIN:	6789

Figure 10.3: IBM method for generating bank card PINs

What goes wrong?
Cat and Mouse games

- Protocol loopholes
- Shoulder-surfing for PIN + discarded ATM slip
- Cameras to get card number and PIN
- Thefts from the mail were also huge
- False terminals
- Biggest threat now are skimmers.



https://www.aliexpress.com/

USA vs EU

- In USA, the Bank pays . 'Judd versus Citibank'.
- In EU, the costumer does. The banks claim it can't be someone else.
- Interesting point is that US banks pay less for security than UK ones, and suffer less ATM frauds.
  - Maybe thieves afraid more from the banks.
- In EU banks not installing cameras because they don't want to admit that ATM's are not immune.(correct to 2008)

Credit Cards

https://www.123rf.com/

Communication Frauds
Cat and Mouse

- First telecommunication fraud at 1836 using Heliograph
- Same difficulties as now:
  - Who do we buy from?
  - Is he trustworthy?

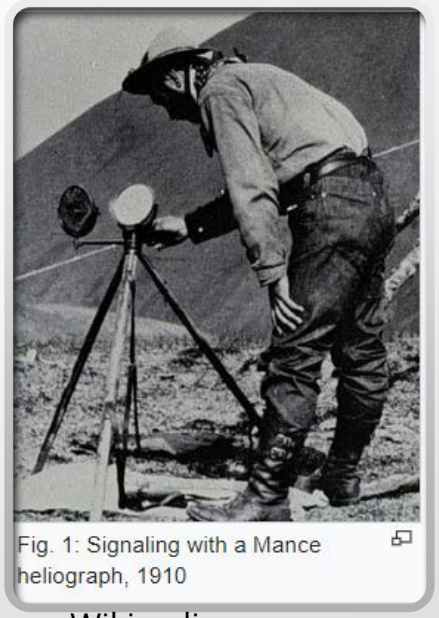
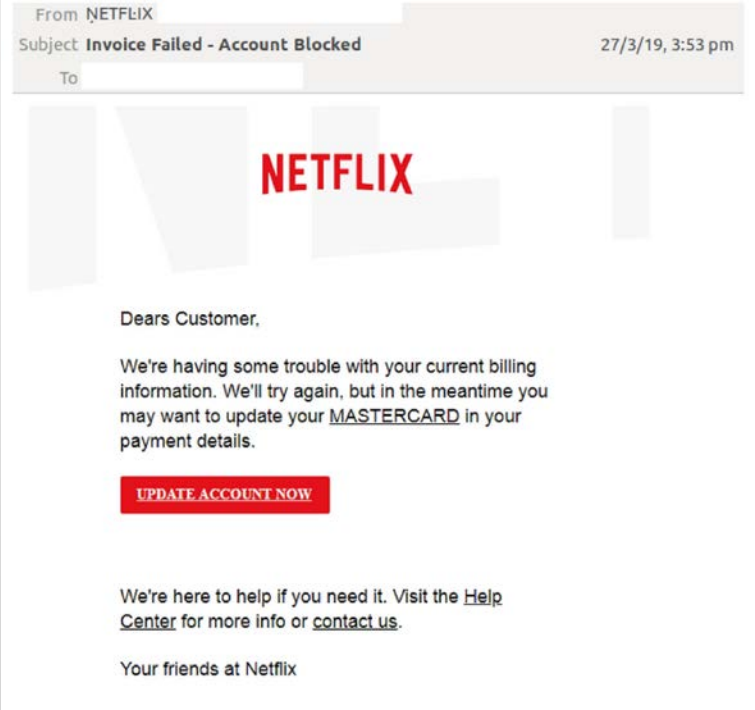


Fig. 1: Signaling with a Mance heliograph, 1910

Wikipedia.com

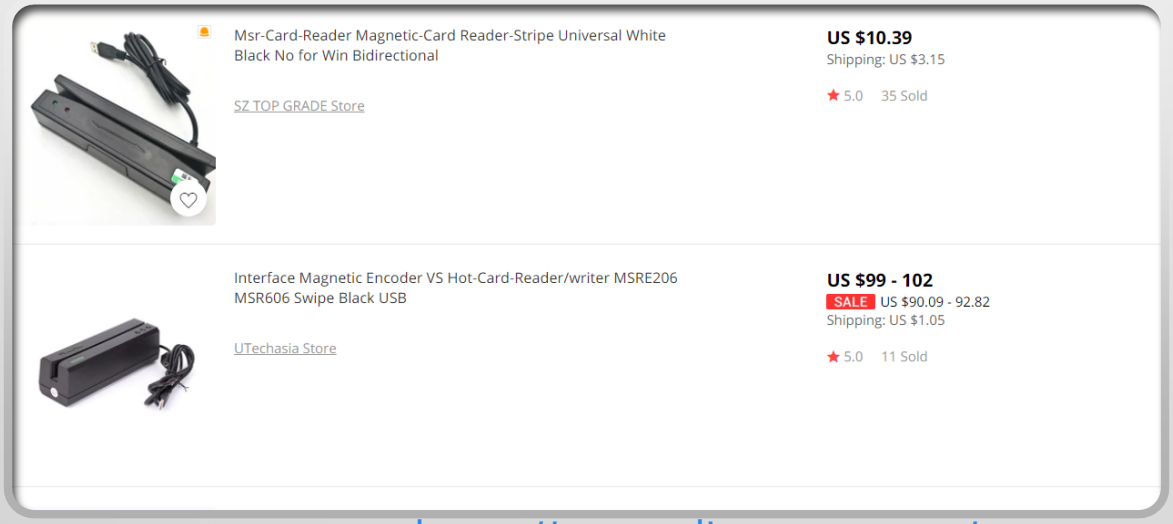
Phishing

Phishing is the fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details by disguising oneself as a trustworthy entity in an electronic communication. Wikipedia



https://www.mailguard.com

Forgery - Cat and Mouse continues



https://www.aliexpress.com/

Forgery - Cat and Mouse continues

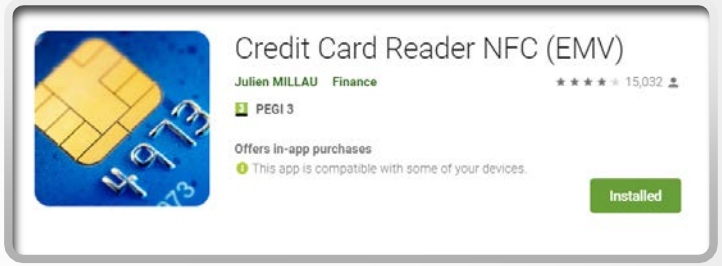
- Crooks could get receipts which where printed with full details, and together with a stolen card(other), they could re encode the card to work.
  - CVV fixed it for a while.
- Crooks went to getting your card details in their businesses, and then a year later you would see a weird bill(now your card details just sold online.)
- Crooks went to skimming

Smartcard-Based Banking-EMV

- Works with certificates
  - First version wasn't fraud resistant as well
  - Shimming, the new skimming
- Has all data of magnetic stripes- can be used for Backward compatibility and used in places that Accept magnetic
- Besides that it is safe . For now…

https://www.cardmachineoutlet.com/products/first-data-fd130-terminal

Smartcard-Based Banking – RFID



https://play.google.com/store/apps

Automatic Fraud Detection

- There are some systems that use purchasing patterns, but unclear how effective they are.
- Businesses, banks try to capture on their own, reward employees- again effective but not long-term solution.
- E-Commerce - nice idea to offer an unreasonable ‘platinum package’.
- E-Commerce - instead of ‘bad card massage’- ‘out of stock’

What should we do?

- Check our credit card statements.
- Be smart online.
- Always be aware when your card is in merchants' hands/ try to avoid in general.
- Look for skimmers, shimmers.
- Spread your knowledge.
- Unfortunately, we are limited in our tools.

What should the banks do?

- Inside Banks:
  - Pay high salaries to employees, especially in key positions . Quick turnovers.
  - Informants rewards
- Outside Banks:
  - Remove the magnetic stripe of credit cards
  - NO physical touch at all, use ATM/Business ID and withdraw from app/special self terminal. Kind of public and private key.
  - Cameras in all ATM's.
  - Approve only regular payments(gas, food). For others use 2FA.

What should the government do?

- Make the banks do what's written in the previous slide
- Make laws that in case of fraud the bank/credit card company, will suffer the lose. This will reduce frauds in general
- Regulate Western Union type of businesses

Questions?

Thank You!