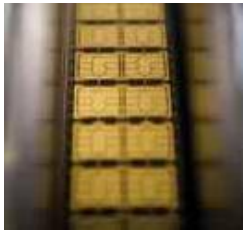
# Smart Card Introduction

## Carte à puce et Java Card

**ATTAC 2011-2012**

Jean-Louis Lanet – Marie-Laure Potet

Jean-louis.lanet@unilim.fr



Université de Limoges

FACULTÉ DES SCIENCES ET TECHNIQUES

# Objective of this lecture

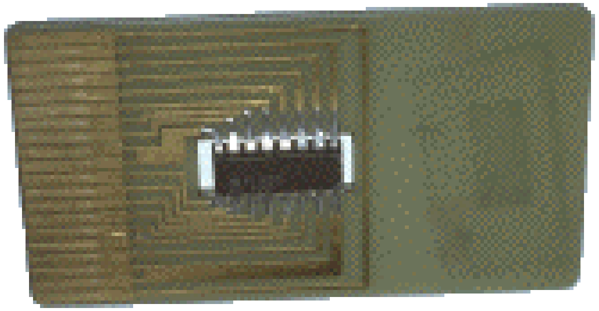
- How to review several technologies within a given application domain.
  - Java, Typed Language, Type inference, Operating System, Security, Smart card fraud, Hardware attacks, Applications : GSM Network…
- Plus some general education :
  - Manufacturing, Companies, Legal issues…

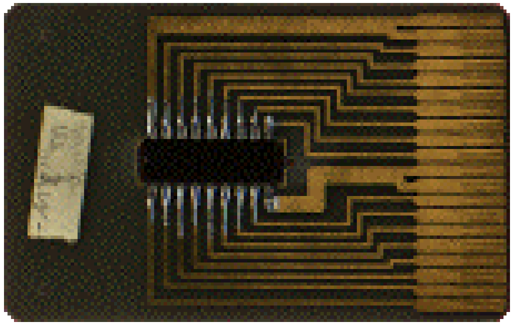
# Agenda

- History
- The industry
- Markets
- Legal Issues
- Smart card a key role against fraud

# History (1/3)

- 1950 Plastic cards in the USA (Diner Club)
- 1960 Magnetic strip
- 1970 Memory card starts
- 1974-1975 R. Moreno replace the magnetic strip by an electronic component (INNOVATRON)





# History (2/3)

- 1979 First microcontroller used in a smart card : Motorola chip by BULL CP8

- Banking cards :
  - 1980: Starting of  “Groupement Carte à Mémoire” (GIE Cartes Bancaires)
  - 1985: First banking card with a microcontroller by Bull CP8

# History (2/3)

- 1984 The French Télécarte
  *"Carte pyjama"*

- 1989 First version of the GSM
- 1994 EMV
- 1997 First Java Card
- 2000 Windows for Smart Card
- 2003-2005 Dot Net Card
- 2006 GemAlto = Gemplus + Axalto
- 2009 GemAlto acquires Trusted Logic, Trusted Labs, Bantry Technology.
- 2011 (september) OCS acquired by Advent

# History (3/3)

- Cartes'96 (CNIT-PARIS)
  - Schlumberger presents Cyberflex 1.0
  - At same time several proposals:
    - Langage C : Multos
    - Langage Forth : Gemplus
  - Smart card manufacturers agreements and Java Card Forum set up.
- 1998 : The real start
  - Cyberflex 2.0, GemXpreso
- 2008 : Next Generation of Java Card : 3.0
  - High end smart card
  - A highly secure KVM.

# Agenda

- History
- The industry
- Markets
- Legal Issues
- Smart card a key role against fraud

# The main actors

- Smart card manufacturers : Gemalto (formerly Gemplus vs. Axalto), Giesecke and Devrient, OCS, Inside secure…
- IC vendors : Infineon, ST Microelectronics, Hitachi, NXP (formerly Philips), Atmel, Samsung…
- Customers : telco, banks, governments…
- Industry consortium (SimAlliance, Java Card Forum,WlanSC,…)
- Other : Sun, Microsoft, Trusted Logics (*R.I.P*) , Security Evaluation center,…

# Agenda

- History
- The industry
- Markets
- Legal Issues
- Smart card a key role against fraud

# Three core markets

## Telecom

**(70% of revenues)**

**Opportunities:**

- Increasing SIM penetration
- Evolving strategic role of the SIM card for telecom operators

## Financial Services

**(20% of revenues)**

**Opportunities:**

- EMV migration gaining momentum

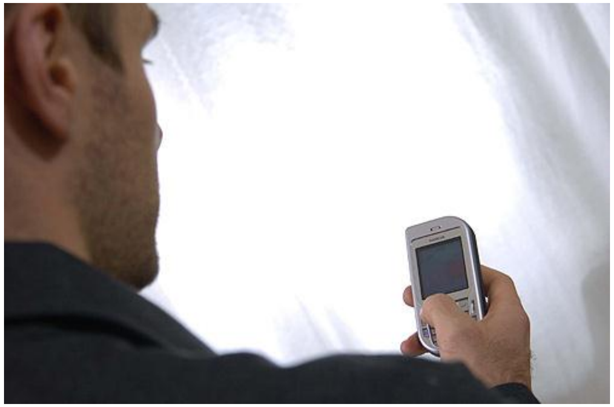
## ID / Security

**(10% of revenues)**

**Opportunities:**

- Emerging high growth market
- Many evolving projects

# Mainstream Applications



Université de Limoges | FACULTÉ DES SCIENCES ET TECHNIQUES

# Emerging apps

# Emerging apps

SUOMI Henkilökortti
FINLAND Identitetskort
FINLAND Identity Card

Sukunimi/Efternamn (1) MATKAILIJA
Etunimet/Förnamn (2) MATTI
Sukup. Kön (3) M
Kortti nro Kort nr (4) 000000000
Kansalaisuus Nationalitet (5) FIN
Synt.aika/Födelsedatum. (6) 01.01.1950
Tunnus/Kod (7) -521X
Myönnetty/Utfärdat (8) 01.06.2004
Viim. voim.olopäivä Sista giltighetsdag (9) 01.06.2009
Haltijan nimikirjoitus Innehavarens namnteckning (10) Matti Matkailija

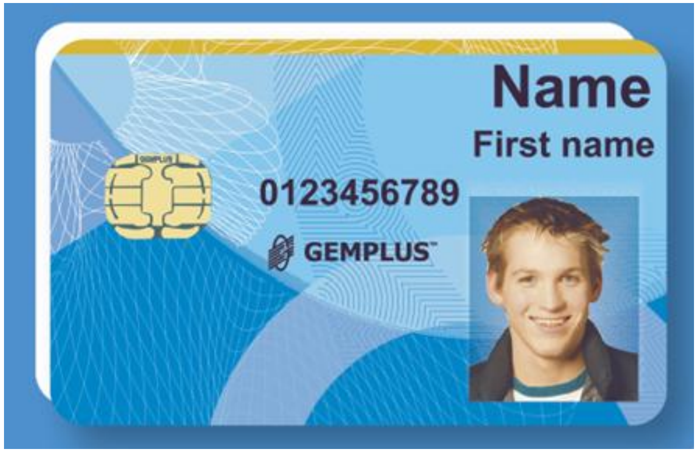
SPECIMEN

VICEMINISTERIO DE TRANSPORTE
DIRECCION GENERAL DE TRANSITO
AV. LAS BUGANVILLAS R-6. COLONIA SAN FRANCISCO
DIRECCION
FEMENINO 1.75 BLANCA VERDES CASTAÑO
SEXO ALTURA PIEL OJOS PELO
0 RH+ ANTEOJOS
T. SANGRE OBSERVACIONES
PENICILINA
ALERGICO A
FERNANDEZ. CARLOS ALBERTO 245-3273 NINGUNA
EN EMERGENCIA AVISAR A TELEFONO MEDICACION PERMANENTE
DIRECTOR GRAL. DE TRANSITO

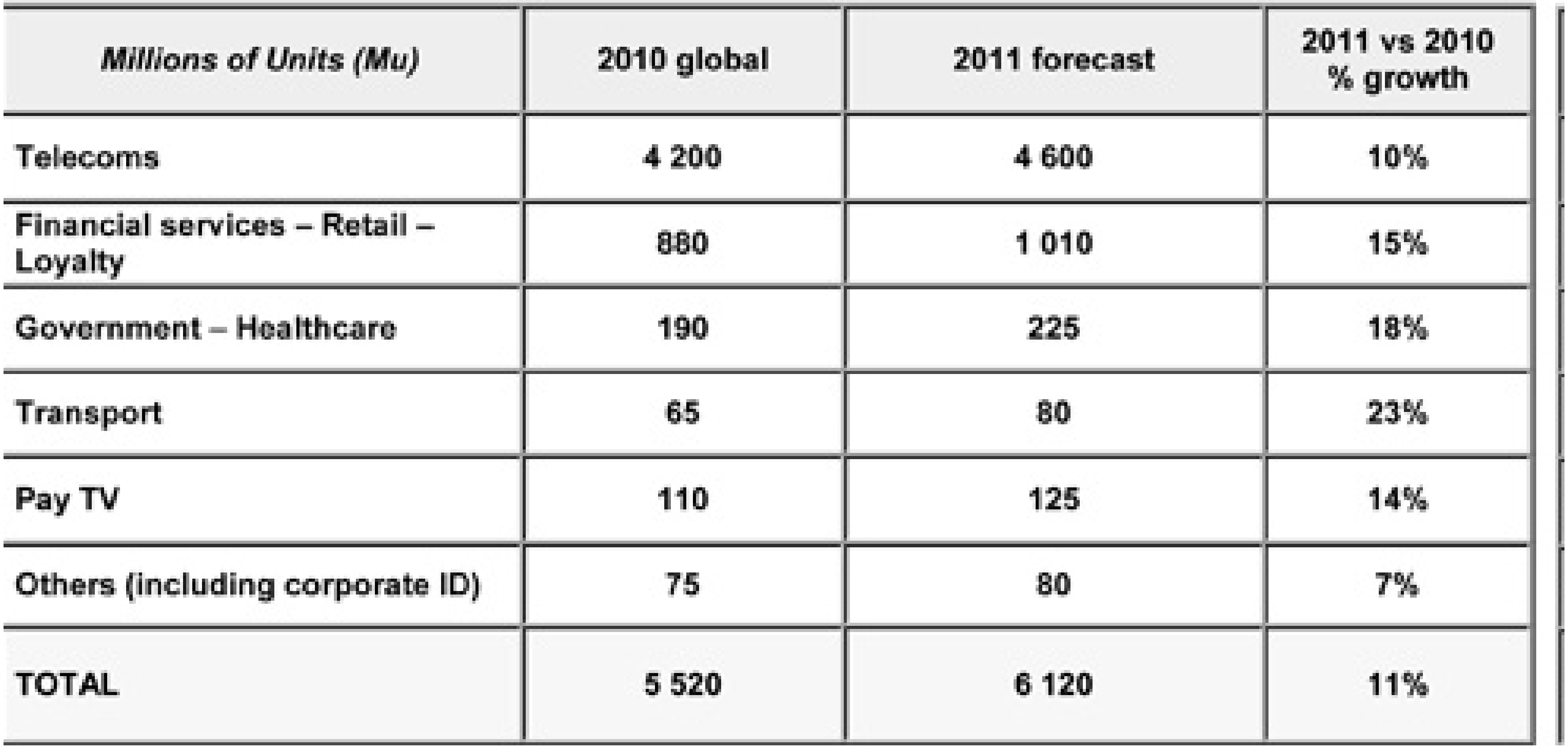
REPUBLICA DE EL SALVADOR
CENTROAMERICA
LICENCIA DE CONDUCIR
Nº LIC: 1234-567890-123-1
PEREYRA ARO. ALEJANDRA LILIANA
PARTICULAR
CLASE
SS-00000210 03.11.1967 04.02.1999 02.11.2003
Nº DE CONTROL FECHA DE NACIMIENTO EXPEDICION VENCIMIENTO

# But also…

moneo

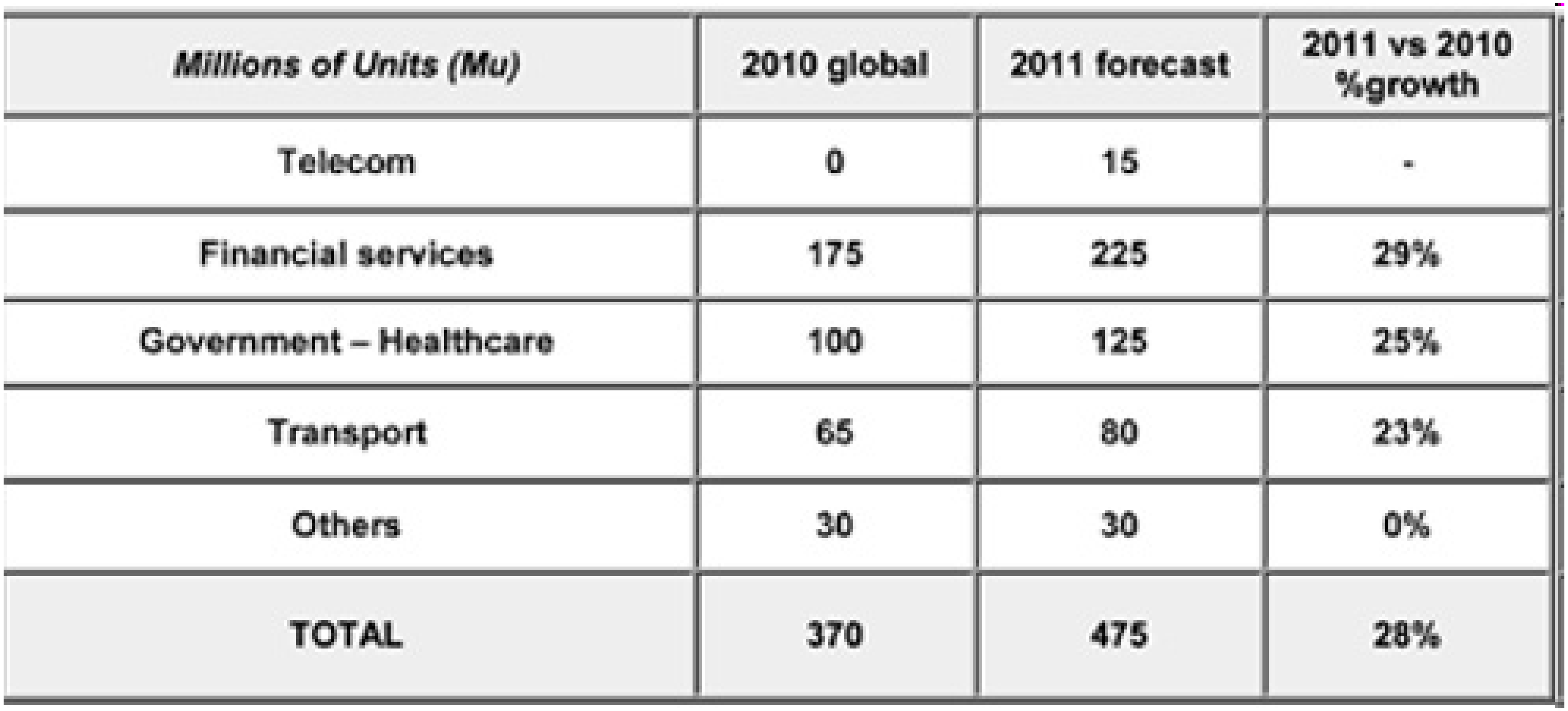


# Some figures (EuroSmart 2011)



| *Millions of Units (Mu)* | 2010 global | 2011 forecast | 2011 vs 2010<br>% growth |
|---|---|---|---|
| Telecoms | 4 200 | 4 600 | 10% |
| Financial services – Retail – Loyalty | 880 | 1 010 | 15% |
| Government – Healthcare | 190 | 225 | 18% |
| Transport | 65 | 80 | 23% |
| Pay TV | 110 | 125 | 14% |
| Others (including corporate ID) | 75 | 80 | 7% |
| TOTAL | 5 520 | 6 120 | 11% |

# Some figures (EuroSmart 2011)



| *Millions of Units (Mu)* | 2010 global | 2011 forecast | 2011 vs 2010 %growth |
|---|---|---|---|
| Telecom | 0 | 15 | - |
| Financial services | 175 | 225 | 29% |
| Government – Healthcare | 100 | 125 | 25% |
| Transport | 65 | 80 | 23% |
| Others | 30 | 30 | 0% |
| TOTAL | 370 | 475 | 28% |

# Some figures

- Smart card costs (2006)
  - Memory cards : 0,15€ to 2€ (for 512 byte to 4 kb)
  - Microprocessor cards :  2€ to 8€ (for 1 à 32 kb)
  - With Crypto processor : 8€ to 16€ (for 8 to 32 kb)

# Why using a smart card?

- It is an object that you own and not a secret that you know,

A password is not an object

# Why using a smart card ?

- It is an object,
- It is personal,

All PC are identical before being sold,
A PC can be formatted, flashed,…

# Why using a smart card ?

- It is an object,
- It is personal,
- It is portable,

My new wallet

A phone cannot be twisted

# Why using a smart card ?

- It is an object,
- It is personal,
- It is portable,
- It is smart,

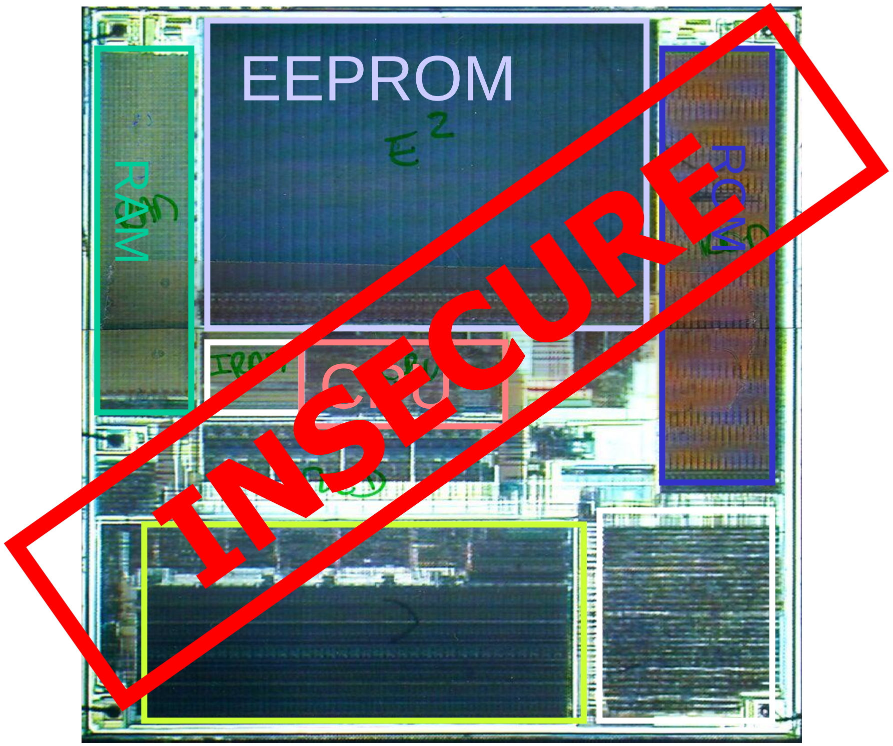
A key don’t know who is using it

# Why using a smart card ?

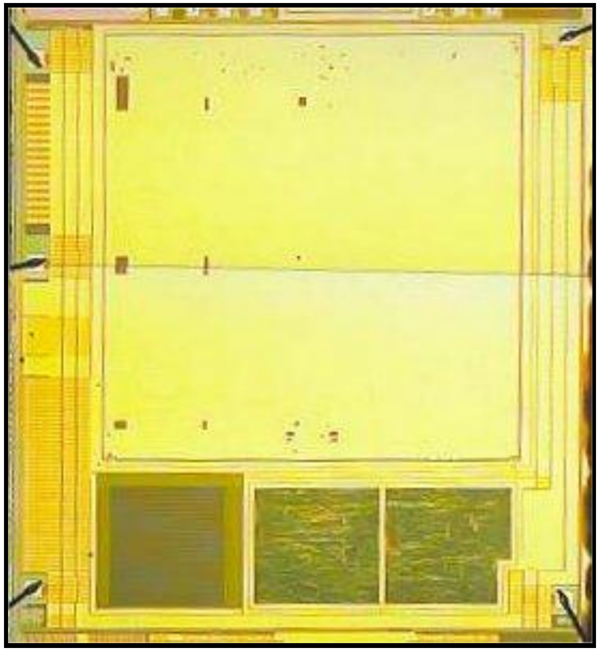
- It is an object,
- It is personal,
- It is portable,
- It is smart,
- It is secure.

Flash memory can be read by everyone

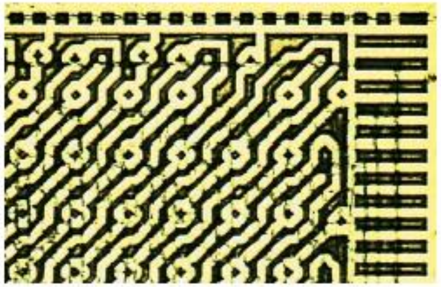
# Layout analysis



- Blocks can be easily identified
- No shield
- No glue logic
- Buses clearly visible



- Shield
- Glue logic
- No Buses visible



# Agenda

- History
- The industry
- Markets
- Legal Issues
- Smart card a key role against fraud

# Attacks

- Smart card is a tamper resistant token not a tamper proof one.
- Attacks to the system can come from
  - Human error (e.g. entering wrong data)
  - Unintentional fraud (e.g. equipment failure)
  - Intentional fraud
    - Misuse of equipment
    - Passive attacks (e.g. listening without modifying)
      - Difficult to detect
      - Preventable
    - Active attacks (e.g. generation, modification of messages)
      - Generally detectable
      - Prevention difficult
  - etc...

# Smart Card Fraud

- Scenario 1:
  - Although PIN protected stolen magnetic stripe credit cards were successfully used to withdraw money
  - Audit of the ATM's log file show that although the thief presented three false PIN code he could somehow get the card back and try again. The correct PIN was found by exhaustive search after approximately 5000 attempts.
- What happened ?
  - After stealing the card, the thief made a small hole in it, attached a wire to full out the card after three false presentation

# Id.

- Scenario 2
  - – Users insert their cards to ATMs enter their PINs but get no money. The ATM swallows the card and display the message “*Invalid card contact your bank*”.
  - – Money was however withdrawn with the card later.
- What happened ?
  - – A false ATM…

# Id.

- Scenario 3
  - Same as the previous one but using smart card with an EEPROM having a retry counter limited to 3. The card is always returned to the user but its EEPROM retry counter never decrease.
  - The audit of the ATM’s log file showed that although the thief presented three false PIN codes he could somehow try again and again. The correct PIN was found by exhaustive search after approximately 5000 attempts.
- What happened ?
  - In old cards EEPROM programming voltage was done using an external programming voltage (Vpp) supplied through a specific ISO contact. The thief had covered this contact with a sticker.

# Id.

- Scenario 4:
  - The ATM’s log file and cash do not match, money is missing
  - Audit of the ATM’s log file showed that the same user withdrew money several times. He always forgot his banknotes that were swallowed back by the ATM after a short time-out (security features)
- What happened ?
  - The thief would withdraw three banknotes but take only two of them. The remaining banknote was detected by the paper sensor and swallowed back by the ATM which automatically cancelled the transaction.
  - The sensor could not distinguish between one, two or three banknotes.

# Id.

- Scenario 5:
  - Users complain that when attempting to withdraw money they get nothing, money is however debited from their accounts
  - An audit of the ATM's log file shows nothing abnormal
- What happened?
  - The hole through which money was delivered was covered by a fake hole (piece of metal)
  - The back of the fake hole was covered with glue to prevent the machine from swallowing back forgotten banknotes.
  - After each victim's withdrawal, the thief would come to the ATM, remove the piece of metal and collect the banknote.

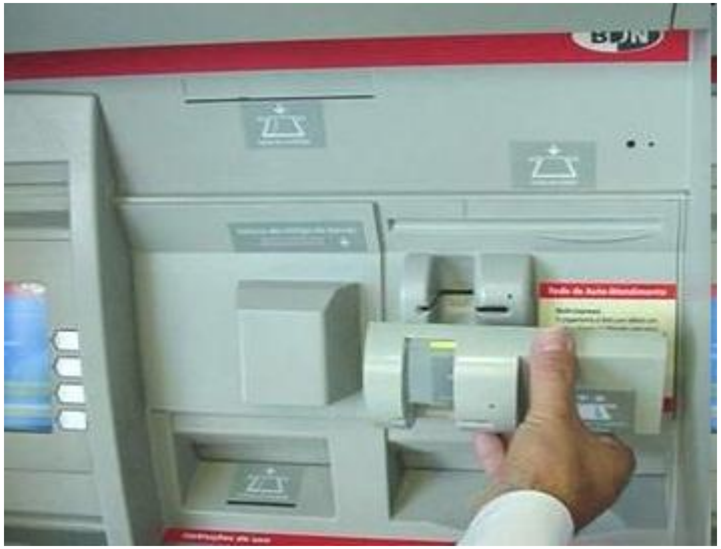
# Skimming

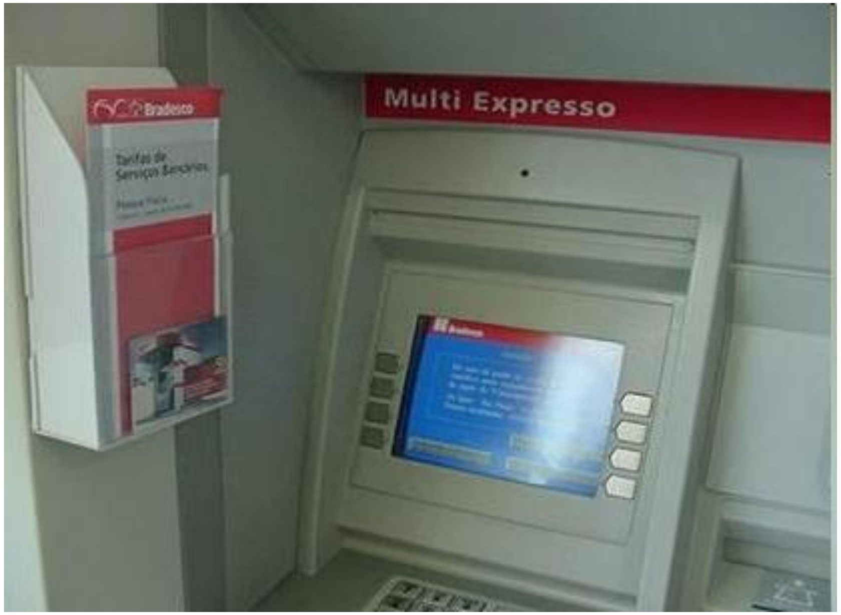
vendredi 07 novembre 2008 : un million retiré sur des comptes de l'Ouest **(Ouest France)**

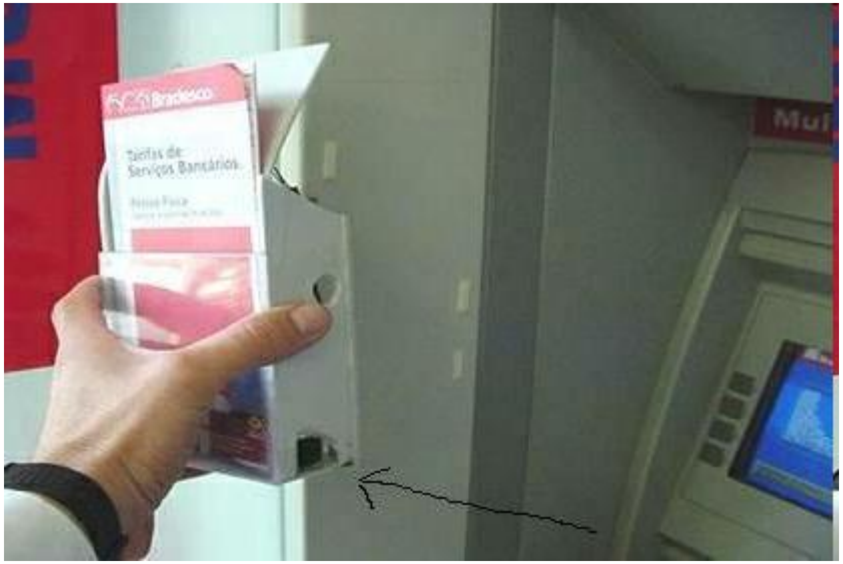
# Skimming

Cout 8k$

- Wifi + sms
- Hong kong, malaisie, USA, France

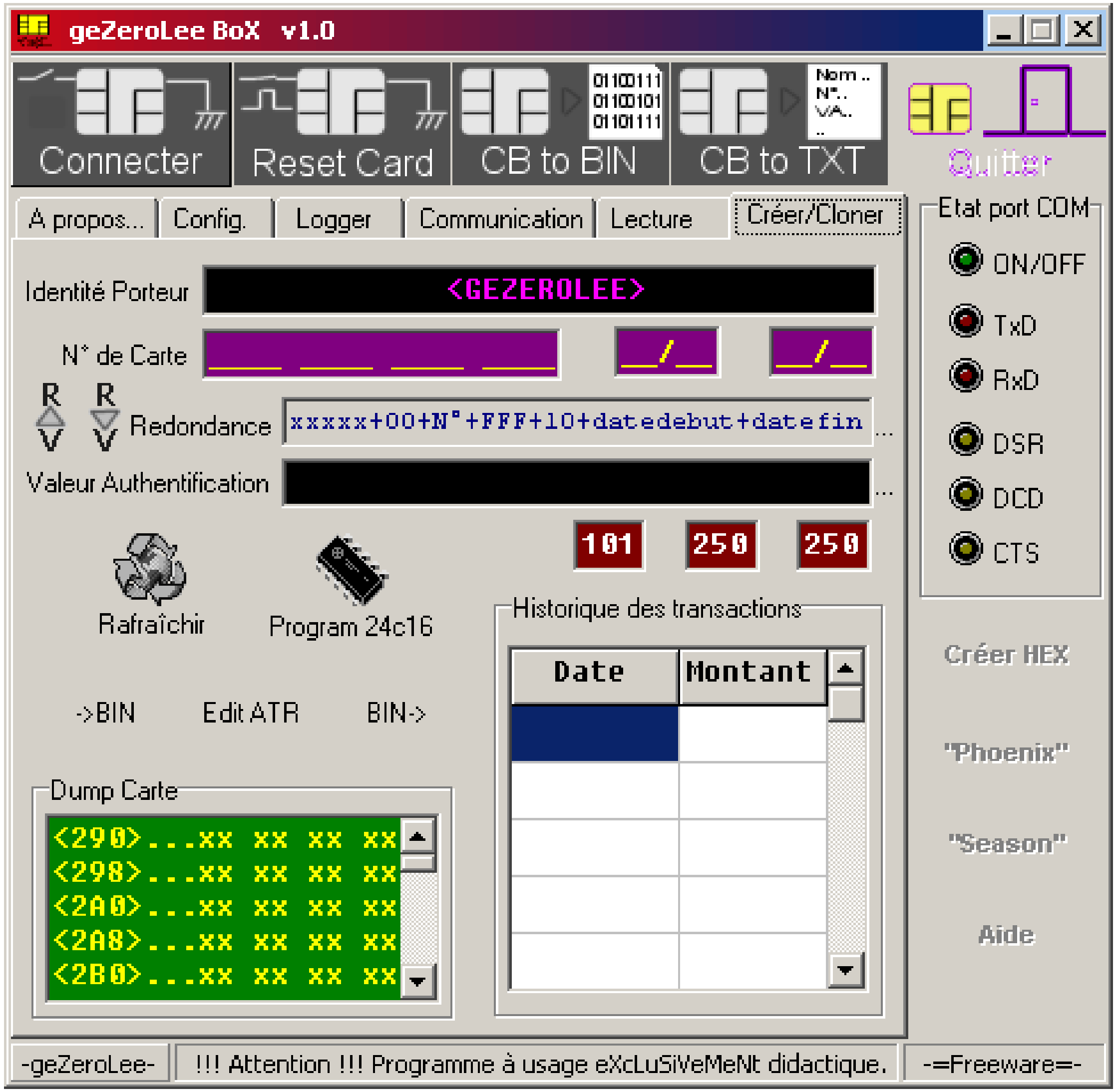






# Id.

- Scenario 6:
  - Although PIN protected stolen smart card were successfully used to withdraw money.
  - An audit of the ATM’s log file shows that the correct PIN was used in the withdrawal operation.
- What happened ?
  - The fraud was technical: the smart card’s software was programmed to compare the presented PIN and if incorrect to increase the EEPROM counter.
  - EEPROM programming is characterized by an increased power consumption and requires 5ms.
  - The thief used a board that presented automatically all the PIN value (0000 to 9999) but detected the current consumption increase and powered off the card before the EEPROM retry counter could be updated.



Identité Porteur: <GEZEROLEE>

N° de Carte: ____ ____ ____ ____   __/__   __/__

Redondance: xxxxx+00+N°+FFF+10+datedebut+datefin ...

Valeur Authentification: ...

101 250 250

Historique des transactions

| Date | Montant |
|---|---|
| | |
| | |
| | |
| | |
| | |

Dump Carte

```
<290>...xx xx xx xx
<298>...xx xx xx xx
<2A0>...xx xx xx xx
<2A8>...xx xx xx xx
<2B0>...xx xx xx xx
```

-geZeroLee- | !!! Attention !!! Programme à usage eXcLuSiVeMeNt didactique. | -=Freeware=-

*Le logiciel G0lee pour la fabrication de Yescard*

# Yescard

- Some details
  - Below a given threshold card and holder authentication are done locally,
  - Only some terminals (gasoline, transport ticket, video rental and so on…) are concerned
    - ATM need always an on-line authorisation
    - Merchant terminal will be detected by the merchant or he/she is himself part of the attack.

# Yescard

- Context
  - – Weakness known by industrial experts
    - Off line authentification : public key
    - On line authentification : secret key
    - Ks stored into the card but easy to retrieve (key was only 320 bits)
    - Cloning a card with forged Vs compatible with  Id
  - – Ended with the court case “Serge Humpich vs GIE-CB.”
  - – Keys have been broadcasted thanks to Usenet.
  - – Card have migrated to EMV 5.1 and  5.2

# Yes Card the protocol

*T → A : « Authentification »*

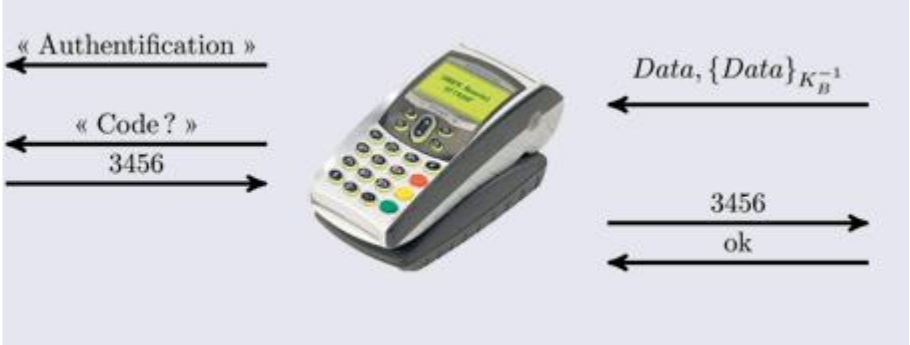
*C → T : Data, {Data}KB-1*

*T → A : « Code ? »*

*A → T : 3456*

*T → C : 3456*

*C → T : ok*



# Yescard

- Consequence
  - Media focused too much on coning Banking Card
    - Moved from a technical risk to industrial image
  - Problem related with knowledge broadcast
    - Know-how used in a fraud context
    - Do we need an internet based *full disclosure*…

# Fraud conclusion

- All this flaws described here are at least nine years old,
- All of them of course have been corrected,
- Security is a permanent race…

# Fraud conclusion

- All this flaws described here are five-seven years old,
- All of them of course have been corrected,
- Security is a permanent race…

**Find a counter measure for the last scenario…**

Any question ?

Université de Limoges

FACULTÉ DES SCIENCES ET TECHNIQUES