What is Smart Cards?
1. What is a smart card?

- Exploded view of a Smart Card
- Architecture of a Smart Card
- Memory Cards
- Microprocessor Cards
- Contactless Cards
1. What is a smart card?

Exploded view of a Smart Card

- Integrated Circuit
  - Free Access Memory
  - Protected Memory
  - Microprocessor

- Plastic Card
  - ABS, PVC, Polycarbonate
    - Hologram
    - Brand Stamp
    - Mag. Stripe

- Micro Module
  - 8 or 6 Contacts

- Chip with antenna

- Contact Smart Card

- Contactless Smart Card
1. What is a smart card?
1. What is a smart card?

Contact Smart Card Standards

- ISO 7816–1: Physical characteristics
- ISO 7816–2: Dimension & location of contacts
- ISO 7816–3: Electronic signal & transmission protocol
- ISO 7816–4: Interindustry commands
- ISO 7816–5: Registration system for application in IC card
- ISO 7816–6: Interindustry data elements
- ISO 7816–7: Interindustry commands for Structured Card Query Language (SCQL)
- ISO 7816–8: Security architecture and related commands
1. What is a smart card?

• ISO 7816 Standards

• ISO 7816-1
  • Dimensions and physical constraints

• ISO 7816-2
  • Electrical signals

• ISO 7816-3
  • Communication protocol

• ISO 7816-4 ...
  • Memory management and inter industry commands
• Free Access Memory card

- Wired Logic: Addressing
- EEPROM: Application Data

• a Memory Card can be compared to a Floppy disk...
1. What is a smart card?

- **Protected Memory Card**

- Wired Logic:
  - Addressing,
  - Security

- EPROM:
  - Security Info.
  - Fuses

- EEPROM:
  - Abaccus counter

- EPROM:
  - Security Info.
  - Application Data

- Wired Logic:
  - Addressing,
  - Security

- EPROM:
  - Security Info.
  - Fuses

- EEPROM:
  - Application Data

- Keys
1. What is a smart card?

Microprocessor Card Architecture

- Clock
- Reset
- Input / Output
- ROM: Operating System
- EEPROM: Application Memory
- CPU
- RAM: Scratch Pad

*a microprocessor card can be compared to a computer!!*
1. What is a smart card?

Processing unit: CPU

• CPU 6805/8051/H8/RISC
• 8 bits/16 bits/32 bits
• 3.57 / 5Mhz
• 5 / 3Volts
1. What is a smart card?

Volatile memory: RAM

- RAM = Random Access Memory
- 128 up to 2 K bytes (Stack included)
- Scratch pad
- Checked and reseted after reset
1. What is a smart card?

Non Volatile memories

- ROM (Read Only Memory)
- EEPROM (Electrically Erasable and Programable Read Only Memory)
1. What is a smart card?

- Operating System
  - I/O protocol
  - Chip handler
  - External commands
  - Memory management
  - Authentication algorithms

- 6 up to 56k bytes
1. What is a smart card?

- Application memory
- Specific file architecture
- Data informations
- Softmask
- Data OS
- 1 up to 64 K bytes
1. What is a smart card?

- Light
- Temperature
- Passivation
- Clock
- Vcc
1. What is a smart card?

- **Integrated Circuits**
  - Power circuit
  - Analog I/O circuit
  - Data storage and processing

- **Power transmission**
  - coil

- **Plastic Card**

- **Data**
  - transmission
  - coil or plates
2. How does a smart card work?

Main Functions of a Smart Card

- Smart card functions
- Mechanical strength
- Data security
- Data storage
- Data processing
2. How does a smart card work?

Functions of a Smart Card

- **1- Token card**
  - Read / write / erase data in memory
  - Protect data (ex: serial number storage)
  - Process certificates: Authentication,…
  - Count units: Abaccos
- **2- Microprocessor cards**
  - Read / write / erase data
  - Identify the card: component,…
  - Manage Memory
  - Manage Files (PC): multi-application cards,…
  - Protect data (ex: secret key storage)
  - Encrypt data (ex: financial transactions)
  - Authenticate (ex: card owner with PIN)
2. How does a smart card work?

Read and Write in a token Card

**READER**
- Electronics
- Connector

**CARD**
- Power, Clock
- RAZ
- Messages
- I/O logic
- X select
3. Manufacturing Process

- Plastic Cards
- Modules
- Embedding & Test
- Personalization
3. Manufacturing Process

Card Body

- ABS / ABS modified
- PVC
- Polycarbonate

- Hologram
- Brand Stamp
- Magnetic stripe
- Printing
• 8 or 6 contacts
  – 1. Vcc
  – 2. Reset
  – 3. Clock
  – 4. (Optional)
  – 5. Ground
  – 6. (optional)
  – 7. Input/Output
  – 8. (optional)
• Metal: Tungsten, Gold
3. Manufacturing Process

- Graphic data
  - (Films, disk, syquest...)

- Punching

- Plastic sheet: PVC

- Sheet Printing

- Sky High Transit
3. Manufacturing Process

Module Assembly Process

- Wafer
- Probing
- Dicing
- Die
- Bonding
- Module
- Coating

- Motorola, Atmel
- Texas Instruments
- SGS Thomson
- Siemens, Hitachi
3. Manufacturing Process

• 1. Punch or mold

• 2. Mill

• 3. Insert

• 4. Test - Serialize

• 5. Personalize
3. Manufacturing Process

- Bank card (mP+magstripe) Personalization Process

- Customer ID file
- Black box
- Mag tape
- Stripe Card
- Embossing
- Encoding
- Mag tape Smart Card
- Microprocessor card encoding
- Personal ID mailing
- Final Inspection and shipping
Main industrial actors in the smart card environment

- Chip manufacturer
  - Motorola, Siemens...

- Printer

- Embedder

- Card supplier

- Card issuer:
  - Bank, Telecom,..

- Terminal manufacturer
  - Verifone, L&G,..

- Processor

- Card Owner

- Service Provider
  - FDR
• Benefits of the Smart Card
• Cards technology features
• Applications
• Exemple of Applications Architectures
4. Applications of the smart card

• Why a smart card?
  • Portable and mobile: identify the owner
  • Convenient and flexible
  • Protected and secure
  • Good mechanical strength
  • Proven technology with good reliability
  • Can store and process data (personal, digital certificates, ..)
  • Cost effective
  • Branded
  • Innovative
4. Applications of the smart card

- Ultra Mall
- Rewards

- Electronic
  - Commerce

- Loyalty

- Electronic Purse

- Access control
  - Network security

- Credit/Debit

- Access Control

- Ticketless Traveling

- Parking

- Pay TV

- Payphones

- Digital Cell. Phones

- Mass Transit

- The Very Big Bank
  - Rich Wealth

- 1234 5678 9012 3456

- Credit/Debit

- Pay TV

- Payphones

- Digital Cell. Phones

- Mass Transit

- The Very Big Bank
  - Rich Wealth

- 1234 5678 9012 3456

- Credit/Debit
4. Applications of the smart card

Smart card in Retail E-Commerce

- **Virtual Mall**: Purchase order via Internet Kiosks
- **Settlement network**: Authorization / Settlement, Reload Terminal
- **Real Mall**: Household, IC card
- **Virtual mall**: Credit card company, Bank
4. Applications of the smart card

Smart Cards in Pay TV

- Emission Center
- Access rights
- Scrambling Keys
- Set up box
- Image Scrambling
- Pay TV
4. Applications of the smart card

- Smart Card in Mobile Phones
- Banking, Trading & Shopping

- •SMS Centre
- •OTAC
- •NetGate
- •GSM
- •Internet
- •Web server
- •Banking server

- •Back
- •Office
4. Applications of the smart card

Smart Cards in Network Security

• Handshake
• Exchange Public Keys & Challenges

• A: Joe Traveler
  • CryptoFlex
    • RSA Engine
      • A Public Key
      • B Public Key
  • Blablabla
  • B Challenge

• B: Global-Travel Agency
  • CryptoFlex
    • RSA Engine
      • B Private Key
      • A Public Key
The French Health Care System

1. Dr Smith
   - Prescription
   - Payment

2. Mr. Martin
   - Professional
   - Social Security
   - CNAM

Smart cards in Health

4. Applications of the smart card
## II. Smart Cards Attack – From ICTK

<table>
<thead>
<tr>
<th>Attack to be considered</th>
<th>Attack Category</th>
<th>Assurance gained by</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Chip Evaluation</td>
</tr>
<tr>
<td>1 Minimal Invasive or Non-Invasive Physical Attacks</td>
<td>Hardware Evaluation</td>
<td>X</td>
</tr>
<tr>
<td>2 Physical Attacks to Retrieve Secret Data</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>3 Overcoming Sensors, Switches and Filters</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>4 Perturbation Attacks</td>
<td>Perturbation Analysis</td>
<td>X</td>
</tr>
<tr>
<td>5 Retrieving keys with DFA</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>6 SPA/DPA – Non-invasive retrieving of secret data</td>
<td>Side-channel Analysis</td>
<td>X</td>
</tr>
<tr>
<td>7 EMA and Sound Attacks</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>8 Exploitation of Hardware Test Interfaces (JTAG)</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>9 Attacks on RNG</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>10 Software Attacks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11 Information gathering</td>
<td></td>
<td></td>
</tr>
<tr>
<td>12 Editing Messages</td>
<td></td>
<td></td>
</tr>
<tr>
<td>13 Direct protocol attacks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>14 Man-in-the-middle attacks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15 Replay attacks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16 Buffer overflow or stack overflow</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Chip Fabrication
Finished wafer
Micro module etching
Automatic etcher
Result of etching process
Silicon Inspection
Reverse engineering
Lay-out plots
IR picture from back
Metal mask ROM

active transistor
disabled transistor
Ion implant ROM after staining
Automated ROM scanning set-up
Sub micron probe station
Probing with eight needles
Probing set-up
Scanning Electron Microscope
SEM: view mode

- primary scanning electron beam
- secondary electrons
- detector
- passivation layer
- chip substrate
SEM imaging
Focused Ion Beam systems (FIB)
FIB - milling mode

- Gallium ion beam
- Milling products
- Secondary electrons
- Detector
Cross-sectioning

focused ion beam
Cross-sectioning
FIB – deposition mode

gallium ion beam

gas injection

gas decomposition

platinum deposition

secondary electrons

detector
Circuit modification

- Conductive strap to be added (white bar)
- Track to be cut (yellow cross)
- Creation of taps
- Change functionality
Fuse repair

platinum overspray
Metal deposition: probe pad
Metal deposition: probe pad
Laser cutter for shield removal

FIB modification after laser modification
Side channel attacks

- Side Channel Leakage sources
  - Power leakage
  - Electro-magnetic leakage

- Simple Power Analysis
  - Timing attacks
  - Waveform attacks

- Differential Power Analysis
  - Application of DPA
  - How DPA is used on DES to extract the key
Power consumption within a smart card

- P-transistor
- N-transistor
- Capacitor (e.g. bus wire)
- Current due to capacitor charge for $0 \rightarrow 1$ output transition
Power consumption of a smart card
Power consumption of a smart card

(internal) current due to capacitor discharge for $1 \rightarrow 0$ output transition

capacitor (e.g. bus wire)
Power consumption of a smart card
Power analysis configuration

digital oscilloscope

PC

control hardware + passive card reader

data

control

power signal to scope

card

I/O
CLK
RST

supply voltage

current flow

resistor

GND
Typical power traces

SW DES

HW DES 4x

ECC
Typical power traces (continued)

RSA Mod Exp

RSA CRT

EEPROM Write 3x
Exercise on bit propagation (1)

Bit propagation in five rounds of DES

Explain the differences between bits 0 and 1:
- why no peaks for bit 1 around sample 2000?
- why peaks for bit 1 at 2500 and for bit 0 at 3700?
- why no peaks after 3700?
Timing Attack on RSA (2)
Electric fields

conductor

electric field
EMA setup in Faraday Cage
Multi-channel Analysis: Clock extraction

- Assume a product with free-running internal clock
- DPA difficult due to bad alignment
- Internal clock signal is prominent in E-M signal
- High order DPA

Diagram:
- Pick-up coil → E-M signal → process → derived clock
  - raw power signal traces → integrate → DPA traces
Power measurement on contactless card
Typical voltage glitching

- Power supply Voltage
- Sense amplifier Threshold
- Bit line voltage
- Ground level

Diagram:
- Memory
- Sense Amplifiers
- Bus
- Descramble
- CPU
Active probing, principle

- Tri-state driver
  - write
- buffer
  - read
- probe needle
- chip
Laser cutter
Perturbation – surface scan with light
Causes of threats (3)

Intrinsic vulnerabilities

- perturbation of CPU
- side channel leakage
- chip modification
- reverse engineering of e.g. ROM code

 Attacks can exploit intrinsic vulnerabilities with impact on asset security