EMBEDDED SECURITY SYSTEMS 2015

Mirosław Kutyłowski

&grades: 40% lecture, 60% lab

exam, no tests during the course, exam in English unless...

short problems, skills examined not knowledge

lower bound: 40% 3, 50% 3.5, 60% 4, 70 % 4.5 80% 5.0

Objectives

presentation of architecture, limitations and functionalities of embedded systems used in security area C2 developing programming skills concerning cryptographic smart cards and FPGA

---

1. smart cards ≈6 hours
2. security printing ≈2 hours
3. telecommunication systems ≈2 hours
4. HSM, TPM, remote attestation ≈4 hours
5. FPGA ≈2
6. sensor systems ≈2 hours
7. RFID tags ≈4 hours
8. CUDA and parallel programming ≈4 hours
9. smart meters ≈2 hours

---

1. **SMART CARDS**

cards of no-smart solutions:

- **embossed** - credit cards: reading does not require electricity, elementary protection only
- **magnetic:** ≈1000 bits, 3 tracks, track 1: 79 6bit chars, track 2: 40 4bit chars, track 3: 107 4-bit chars, limited density (movement in reader against the head), standard data on tracks 1 2, track 3 for read-write, no physical protection, cheap readers, accidental erasure by a nearby magnet, horror as ATM cards (obsolete in EU but still in use in some countries)

  data stored in financial cards: **Track 1**, Format B:

  - start character
  - format character
  - PAN - primary account number — up to 19 characters. e.g. credit card number
  - separator character
  - name: 2 to 26 characters

- separator character ('^')
- expirationYYMM.
- service code 3 characters
- discretionary data: may include Pin Verification Key Indicator (PVKI, 1 character), PIN Verification Value (PVV, 4 characters), Card Verification Value or Card Verification Code (CVV or CVC, 3 characters)
- end sentinel (generally '?')
- one character validity character (over other data on the track).

smart cards: classification

- memory cards (with security logic and without)

  usually memory: non-volatile EEPROM, serial communication, control logic: where you can write. Cheap. E.g. prepayed telephone cards
- processor: with coprocessor or without (as bad as: RSA in 20 minutes)
- contact or wireless

processor cards:

I/O ——— CPU —- flash memory

RAM

ROM

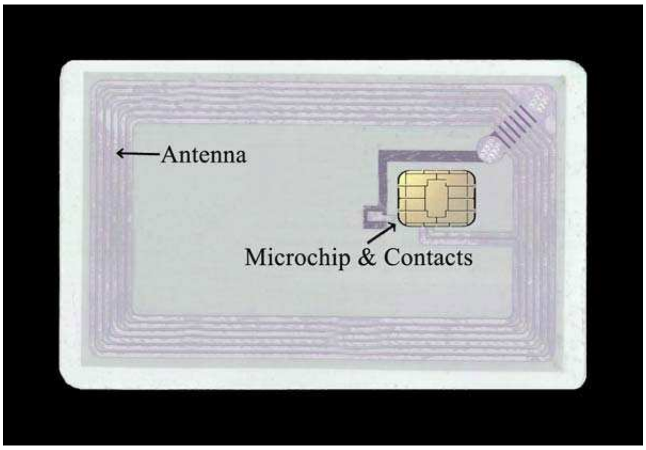
|

NPU (numerical processing unit)

Contactless cards:

- energy: inductive (low!)
- small range (typicaly 10 cm)
- a reader may activate it from distance
- response with low energy, recognizable from a short distance only
- memory: kilobytes
- well sealed against corrosion
- main parts:
  - antenna (most area of the card)

- electronic part: modulation, demodulation, clock generator, voltage regulation, reset generation
- interface between RF interface and memory chip
- access logic
- application data: EEPROM, ROM



contacts:

- 8 fields, normally 6 used (2 for future applications), places for contacts strictly determined in standard
- 8 connections, 2 auxiliary and can be omitted or used e.g. for USB

  connections:

  - C1: Vcc voltage supply
  - C2: RST reset
  - C3 CLK clock
  - C4 AUX1
  - C5 GDN ground
  - C6 SPU standard or proprietary use (SWP)
  - C7 I/O
  - C8 AUX2

  ––––––

  |C1 C5 |

  |C2 C6|

  |C3 C7|

  |C4 C8|

  ––––––

- easy to destroy
- corrosion, mechanical scratches, not for intensive use

security tokens:

- type 1: USB tokens – contact interface like in USB, insert into a port after breaking out of a card
- type 2: small display (eg. 4 digits). input also possible: e.g. a card with 2 buttons (each one side of the card), battery inserted

optical:

- writing technique - like CD (linear and not circular)
- area designated field according to standards, may leave place for contact interface of a chip and magnetic strip, less place for graphical part on the card
- megabytes (≈6MB storage)
- redundancy, therefore not easy to destroy information
- usage: e.g. border control cards (Mexico-USA)

Physical properties:

standard format: 85.6x54 mm (ID-1), other formats for SIM cards (in larger ID-1 cards with stamping),

parameters:

- mechanical robustness (card and contacts)

- temperature resistance
- surface
- electrostatic discharge
- electromagnetic susceptibility
- ultraviolet radiation
- X-ray radiation

Material: trade-off with different properties

PVC: polivinyl chloride, credit cards, cheap, problems with low and high temperatures, injection molding impossible, lifetime 2 years, cost factor: 1

ABS: a common thermoplastic polymer, mobile, termally stable up to 100 C, laser engraving poor, lifetime 3 years, cost factor: 2

PC: polycarbonate, ID cards, durable, 160 C, problems with hot stamping, lifetime 5 years, cost factor: 7, low scratch resistance,

PET: health cards, mechanical: very good resistance, lifetime 3 years, cost factor: 2.5

Electrical properties:

- max 60 mA for 5V, max ambient temperature 50 degrees**,** 350 $\boldsymbol{\mu A}$ per megaherz, power consumption too low to cause overheating, power reduction e.g. for SIM in different phases of activity (low if the phone is not transmitting and using cryptoprocesor)
- contact C6 was for EEPROM erasing but not needed anymore, used for Single Wire Protocol
- voltage is a problem: 3V for SIM cards (batteries for smarphones weight optimization), 5V needed for EEPROM erasure. charge pumps applied
- no internal clock supply (this is a potential risk: adversary may increase the clock frequency to create faults, fault cryptanalysis)
- problems with collisions on I/O line (too high currents would destroy interface components)
- protection against out of range voltages, electrostatic charges, precisely defined activation and deactivation sequences: first ground, then voltage, then clock, warm reset when voltage increases on the reset line

Chip modules:

- the chip too fragile and too thick to be laminated on the surface. the chip is inserted inside

- electrical connections are the problem, automatic bonding of the gold wires to the back of contacts with ultrasonic welding
- Chip-on flex modules, stages of production:
  - tape with empty modules
  - gluing the dice into modules
  - bonding the dice
  - encapsulating the dice
- lead-frame: chip produced together with contacts and the simply inserted by a robot into the card body and glued

Microcontrollers:

- area: manufacturing costs and durability (bending, torsion), typically 10mm^2, square shape
- must be integrated, "standard components" are not well suited due to size of the resulting circuit,
- native designs are proprietary, even a crime to check the layout
- semiconductor technology -> density increases -> chip area drops . But some problems: error probability, necessity to decrease voltage, ...
- extremely high reliability needed. So behind the "state-of-the-art" which is frequently instable
- memory small (e.g. 100KB), a 8-bit processor ok for less than 64KB, then extensions, usually CISC (complex instruction set computer) - instruction over a number of steps, some based on RISC (reduced instruction set computer), also 32 bit processors that needed also for interpreter based architectures (Java Card)

MEMORY

Memory types:

non volatile:

EPROM - UV erasure, not suited for smart cards,

EEPROM - electrical erasure, cell capacitors, discharged state=0, charged state=1, erase state -> non-erased (single bit), non-erased-> erased: page or sector, both slow, size 1.14 μm, 100.000-1.000.000 erasures, 2-10ms, tunneling efect - if there are electrons on the floating gate then they prevent flow in the substrate

flash - a different technique for writing: hot electron injection, write time „flash", erase like EEPROM, size 0.47, 10.000-100.000 erasures, very fast writing, lower voltage (12V) than EEPROM (17V), NOR flash: free read of individual cells, but complicated circuits, or NAND flash: dense but reading full blocks