Hardware Security

Organisational stuff

Digital Security

Radboud University Nijmegen

TRU/e Master in Cyber Security

Other faces you'll see

Lejla Batina
lectures on side-channel analysis

Omid Bazangani
side-channel assignments

Ileana Buhan

lecture on advanced SCA

This course: topics

- **Smartcards**
  - The prime example of ‘secure’ hardware today
  - *The* standard solution for authentication if username/password is not secure enough
  - Smartcards have a long evolution in attacks and countermeasures

- **Attacks & countermeasures.**
  esp. side-channel attacks

- Applications: EMV & internet banking
- Newer hardware security solutions: TEEs

Other kinds of secure hardware & attacks

Other forms of secure hardware we won't look at (much)

- HSM (Hardware Security Modules)
- TPM (Trusted Platform Modules)
- TEE (Trusted Execution Enviroments)
- PUFs (Physically Uncloneable Functions)
- biometrics?

Other attacks on embedded systems that we won't look at:

- JTAG – debugging interface for all sort of electronics
- reading or modifying firmware
- cold boot attacks to extract data from RAM
- …

This course: form

1. lectures & some reading material
2. group JavaCard smartcard project
   in groups of 4 students
3. side-channel lab assignments
   4 assignments, 3 in pairs & 1 individually?
4. virtual event with hardware security evaluation lab Riscure

Grade based on 2 & 3:

60% group project + 40% side channel lab

JavaCard smartcard project

- **Building smartcard system**
- **Goals**
  - **experience the whole process from high-level design, given security requirements and assumptions, down to actual code on real hardware**
  - **appreciate complexity & interplay of**
    - **design considerations & constraints,**
    - **key management & distribution,**
    - **protocols,**
    - **silly hardware limitations, weird crypto padding,...**
    - **practicalities of *getting all this working*,...**

JavaCard smartcard project

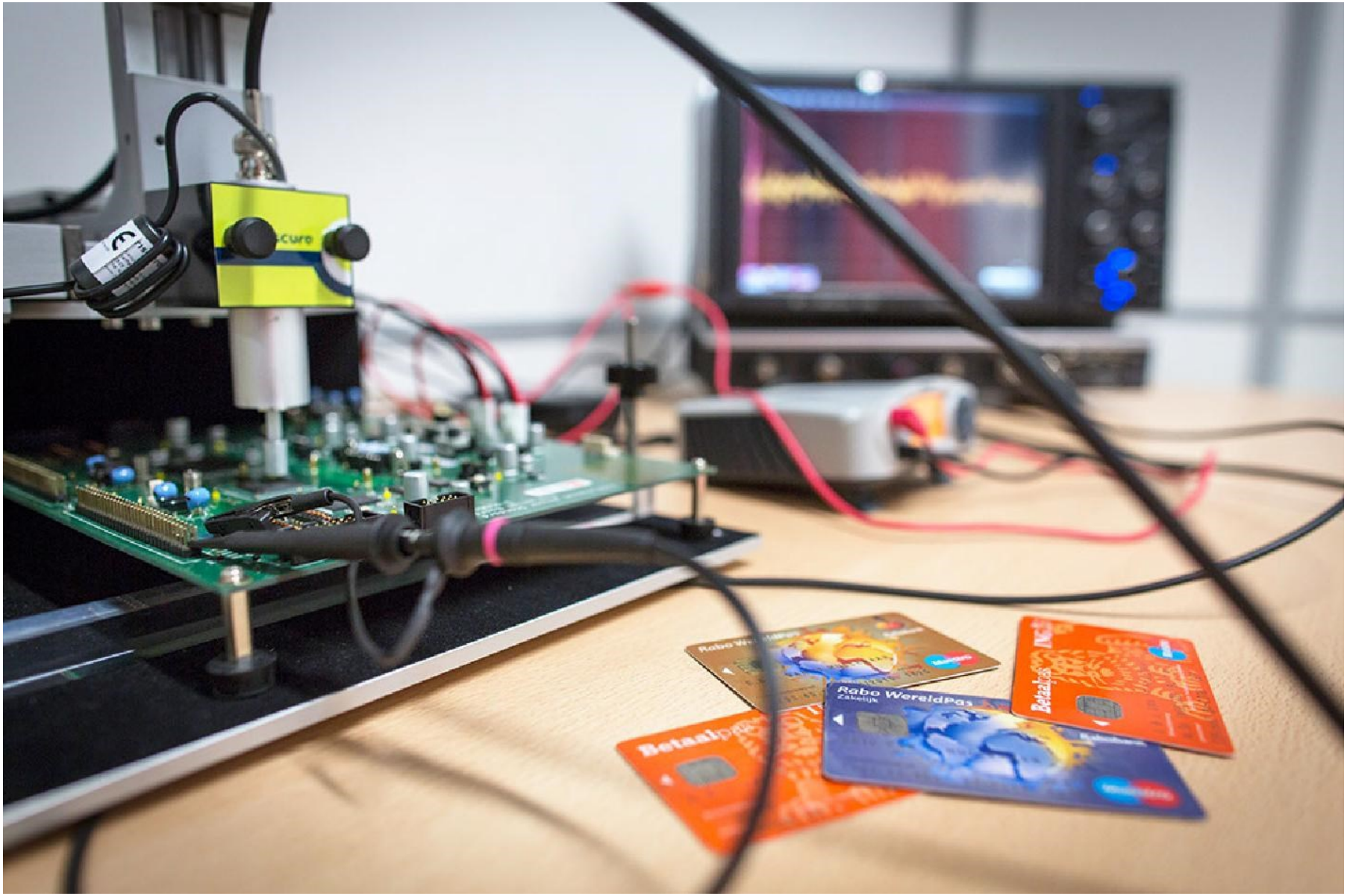
Four choices

1) electronic purse
2) loyalty card
3) petrol rationing
4) car rental

- **Form groups of 4 persons asap**
  - also let us know any group problems asap!!

Side-channel lab assignments

- Practical experience with very successful method of attack on smartcards: Power Analysis


Rabo WereldPas
Zakelijk