The Smartcard OS Company

Light attacks, an intuitive approach

Raphaël BAUDUIN

EDSI presentation

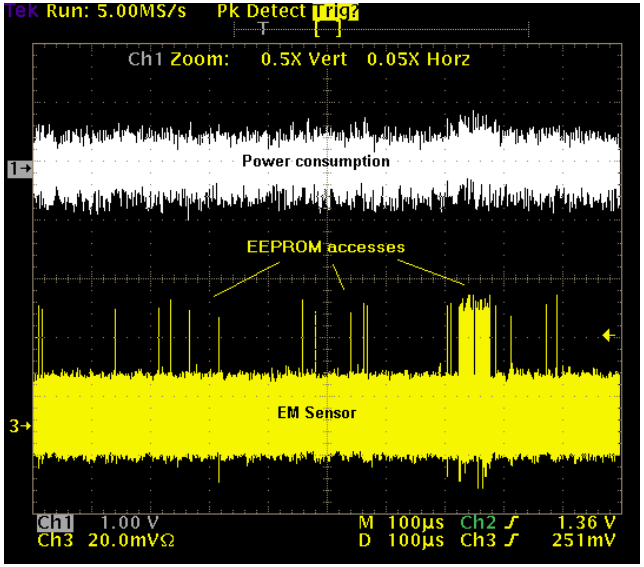
- **French Society created in 1995**
- **2 major activities**
  - Design of Secure Smart Card OS in Cesson-Sévigné R&D Center (25 people)
  - Smart Card Security Evaluation in Caen laboratory (4 people)
- **Customers**
  - Component and OS developers
  - Banking, GSM and Pay TV

Laboratory activity

- **Black box Smart Card Security evaluation**
  - Smart Card specification and samples
  - No information on OS or component security features
- **Reverse engineering of unknown cards**
  - Hacker smart card for Pay TV
- **Expertise on hardware and software security mechanisms**

Test Methodology (1)

- **Analysis of card specifications**
  - Identification of potential attack paths
- **Analysis of card behaviour by passive techniques**

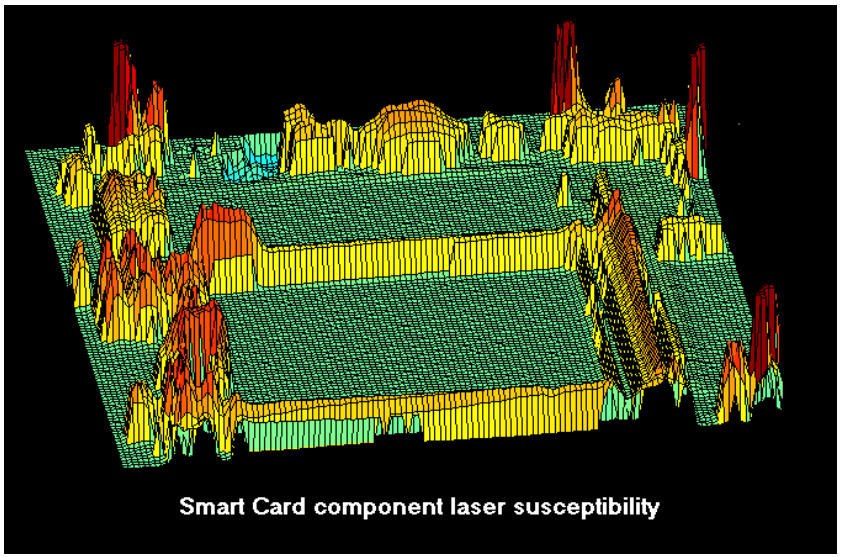


- Power and EM analysis
- Identification of real time synchronisation means to perform perturbation attacks (signal processing)

Test methodology (2)

Analysis of card behaviour by active techniques

- Component susceptibility to different kinds of perturbations (light, EM, glitches)
- Perturbation effects on different areas



- Memory areas (Ram, Rom, Eeprom)
- CPU, Coprocessors
- Security mechanisms (Power scrambling, Internal clock, etc…)

Test methodology (3)

- **Performance of attacks**
  - Passive attacks using SPA and EMA techniques
  - Perturbation attacks

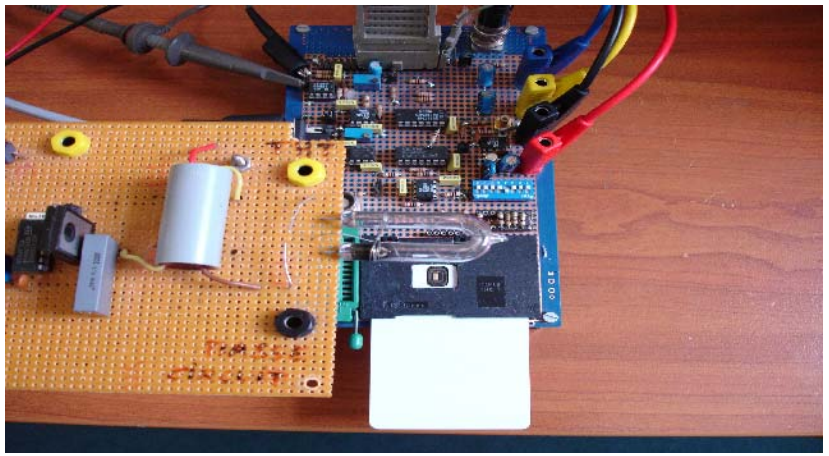
- **For more than 10 years, EDSI develops an important expertise on fault attacks based on light injection**

How to disturb a smart card

- **The energy level must be sufficient and adjustable**
- **The illumination must be temporary**
  - Smart cards often perform integrity checks at reset or later
  - The perturbation must be undetected
- **The illumination has to be located on some parts of the component**
  - Faults induced in different logical functions (RAM, ROM, EEPROM, CPU,…)

Historical perturbation device : a flash lamp

- High energy level is available (several Joules) and illumination can be easily adjusted by moving the lamp up or down
- The flash can be triggered at a precise time by an external signal
- The component's area to illuminate can be selected by masking with paint other areas



Advantages and drawbacks of flash lamp

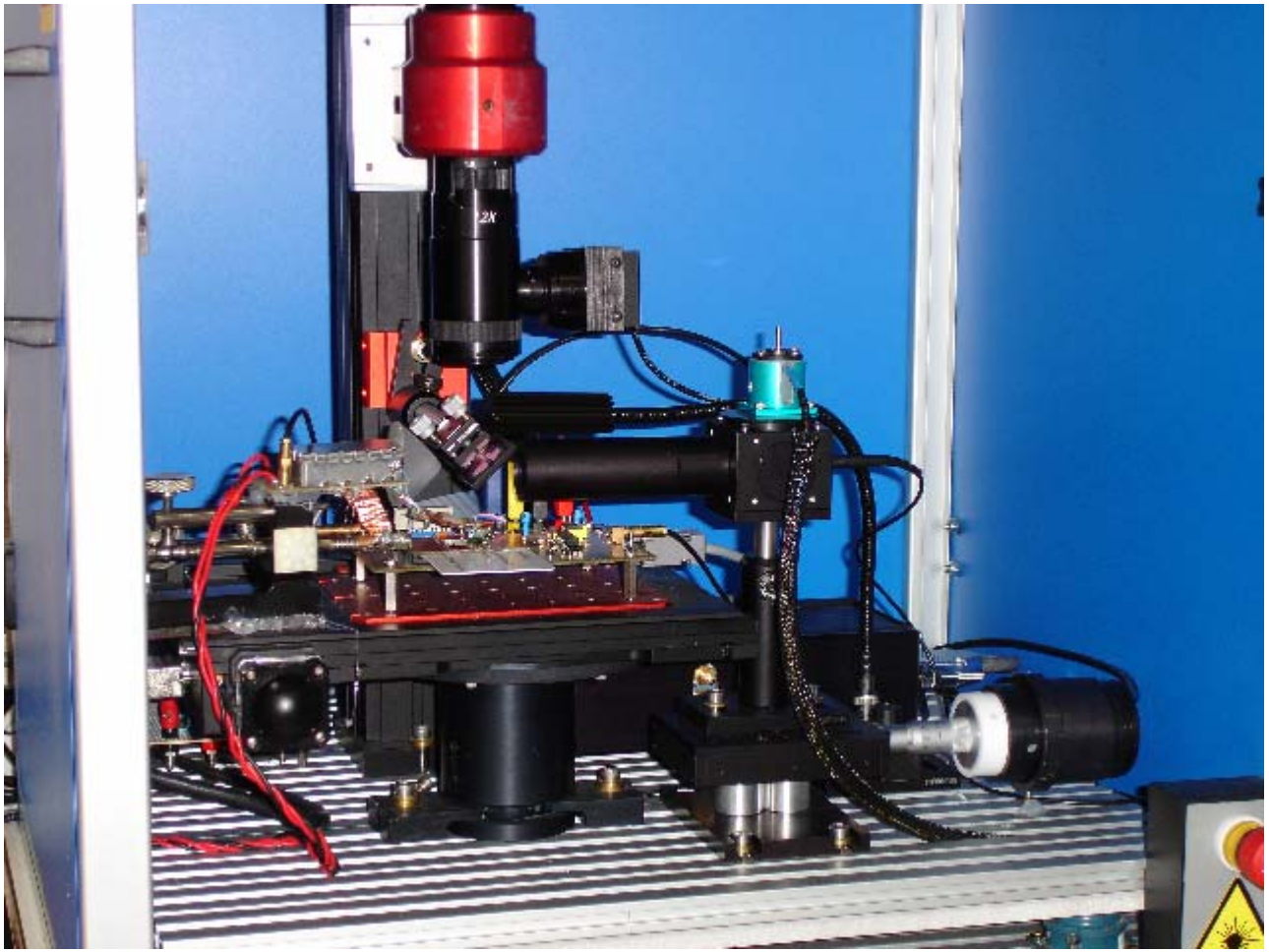
- **Advantages**
  - Price is very low
  - Easy to use
- **Drawbacks**
  - Illumination time is not controled
  - Repeating rate is low
  - Masking unwanted parts can be difficult

A more flexible perturbation device : a laser source

- **With the appropriate source, the laser palliates the flash lamp drawbacks**
  - The illumination time can vary from 10 nS to continuous wave
  - The repeating rate can be as high as wanted
  - The power level can be finely adjusted
  - A collimator can be designed to obtain either a big laser spot or a small one depending on area to illuminate

The Smartcard OS Company

Present laser test bench



Light attacks on today components: Example 1

- Highlighting EEPROM writings with a constant wave 20 Watts halogen lamp via the back side

PICTURE REMOVED

Light attacks on today components: Example 2

- Bypassing EEPROM writings with a 300 nS laser pulse on back side

PICTURE REMOVED

Light attacks on today components: Example 3

- Forcing external clock mode with a 300 nS laser pulse on back side

PICTURE REMOVED

The Smartcard OS Company

Rely on expertise