FIPS Physical security conference, Hawaii 2005

Adequate physical security requirements

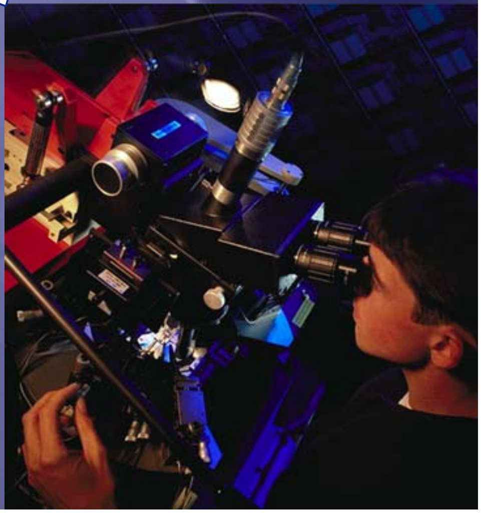
TNO ITSEF

Jan Blonk

TNO ITSEF

www.itsef.com

Blonk@itsef.com



TNO ITSEF

“IT Security Evaluation Facility”

- TNO is an independent R&D company in the Netherlands
- ITSEF is owned by TNO
- TNO ITSEF provides services for:

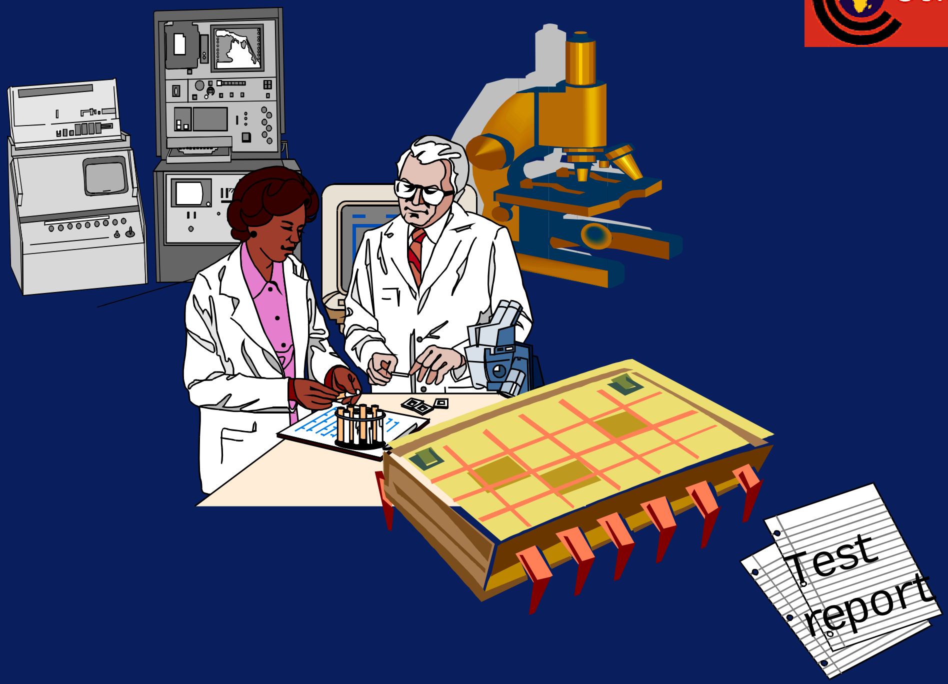
  -security evaluations

  -developer support services

- ITSEF has strict procedures for maintaining client secrecy of sensitive information

Chip security evaluations

TNO ITSEF performs chip evaluations according to different schemes (VISA, MasterCard, CC)

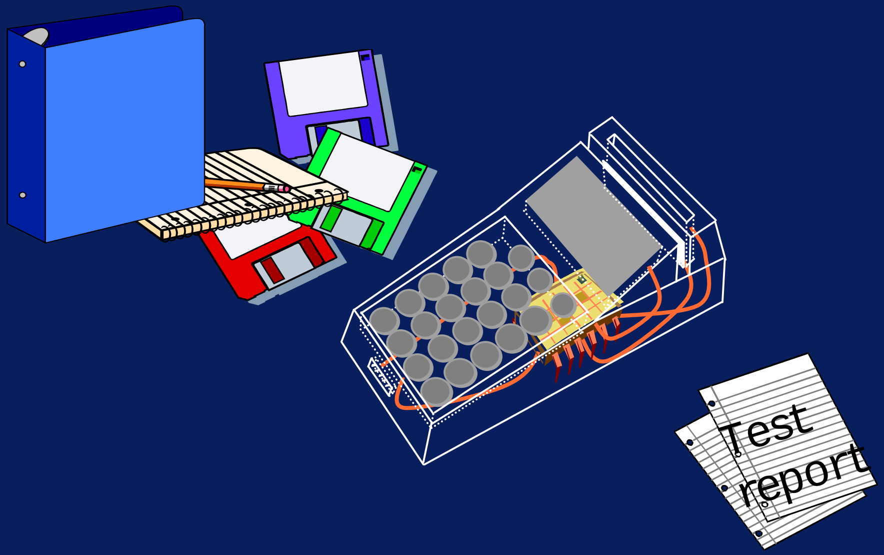


Smart Card security evaluations

TNO ITSEF performs formal and informal evaluations on smart cards with GlobalPlatform or proprietary OSs according to different schemes (VRIR, CAST, CC, other)

Terminal security evaluations

TNO ITSEF performs formal and informal security evaluations on payment terminals according to different schemes (PCI/PED, CC, other)



Approaches for security requirements

Physical security requirements can be given at:

- High abstraction level

  -driven from threats, assets and security level

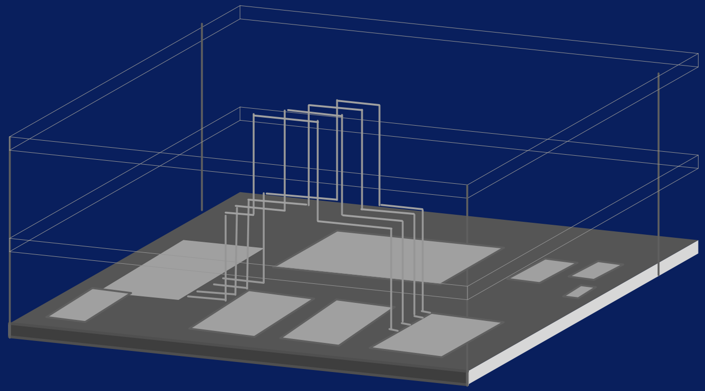
- Technical level

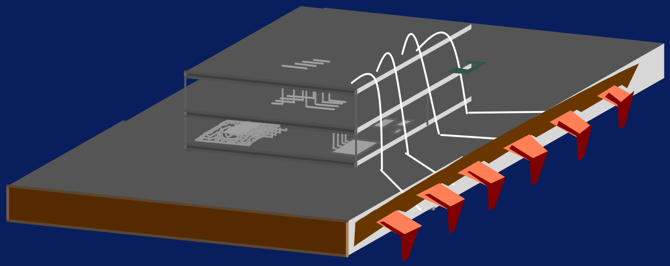
  -driven from generic models

Single chip crypto module

Possible attacks:

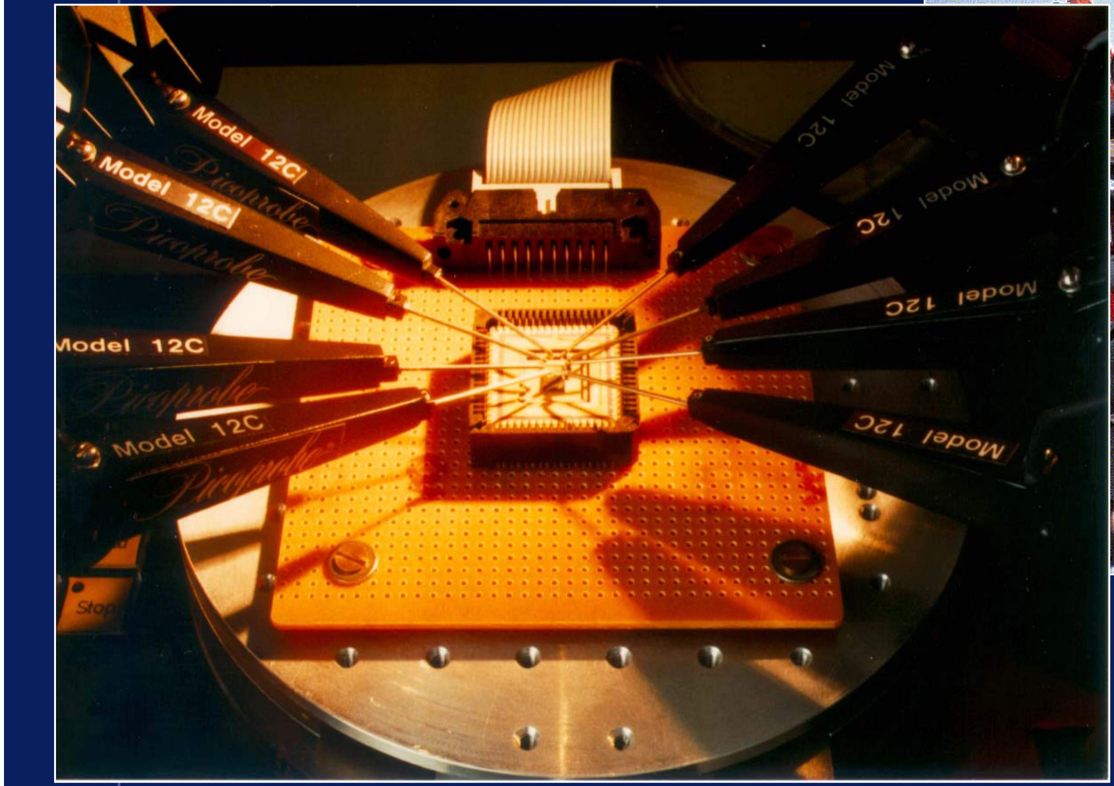
- Internal attacks
  - Observation
  - Chip modification
- Side channel attacks
  - SPA/DPA
  - EMA/DEMA
- Perturbation
  - Light
  - Excess voltage
  - Voltage glitches
  - Temperature





Internal attacks

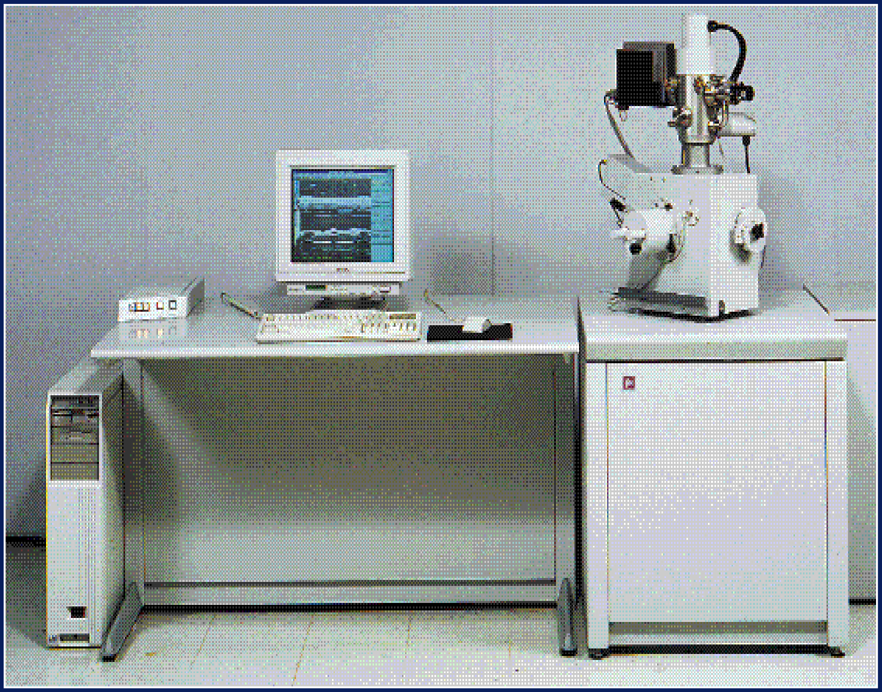
Access chip wires with micro probe needles

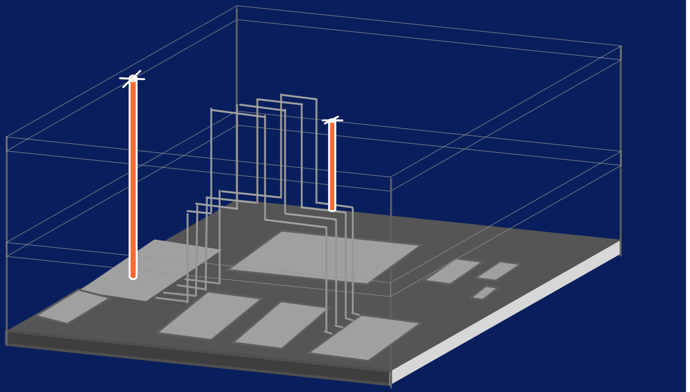


Internal attack

Modify chip with a Focused Ion Beam

- access wires in lower layers
- cut wires in lower layers

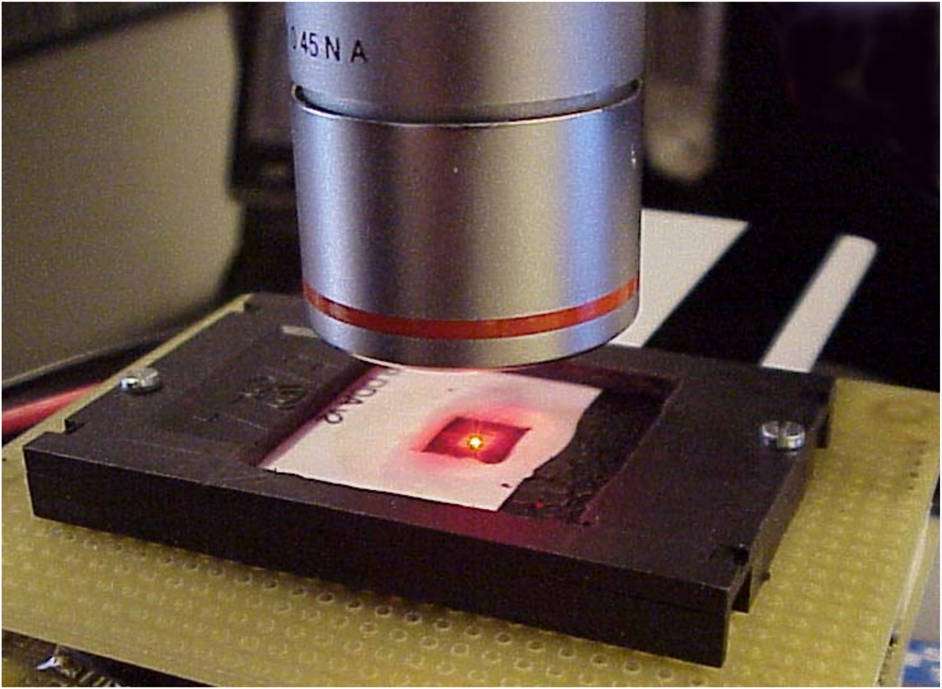


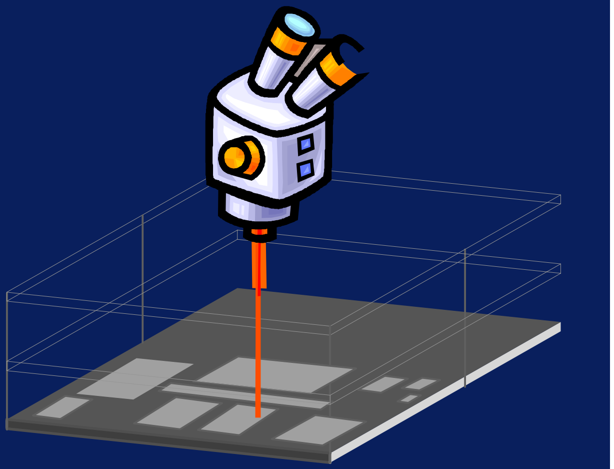


Perturbation

Light attack

- Transistors are susceptable to light
- Changes in instruction processing





Example of Security levels

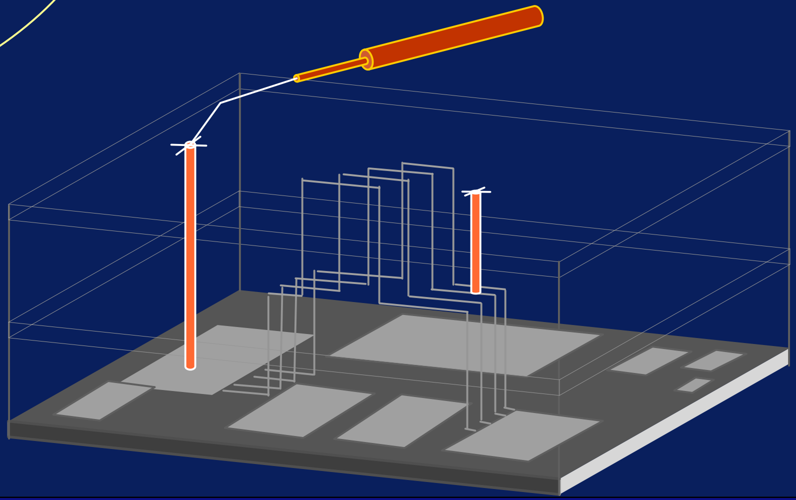
Chip must have protection against:

1. Attack on surface
2. Reverse engineering of design
3. Memory data read
4. Access to buses
5. Physical modification
6. Information extraction

Level1

Level2

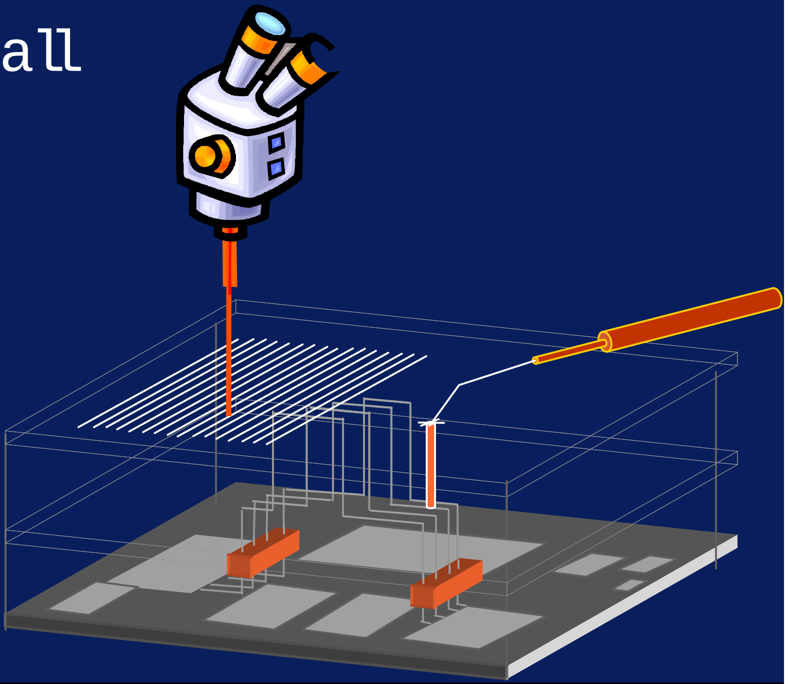
Level3



Security Levels abandoned

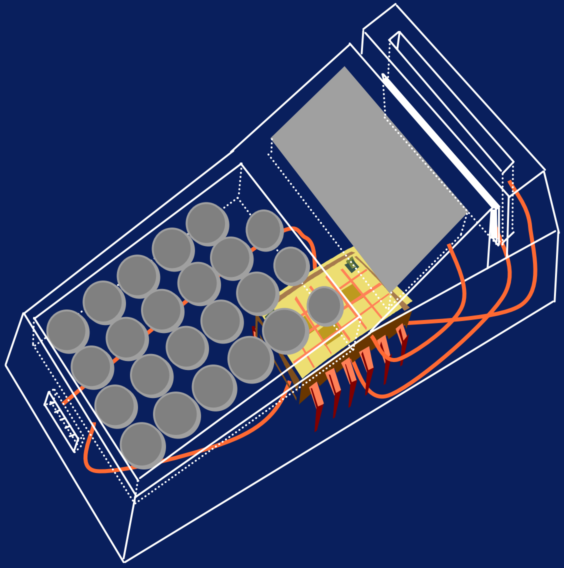
Reasons for abandoning leveled model:

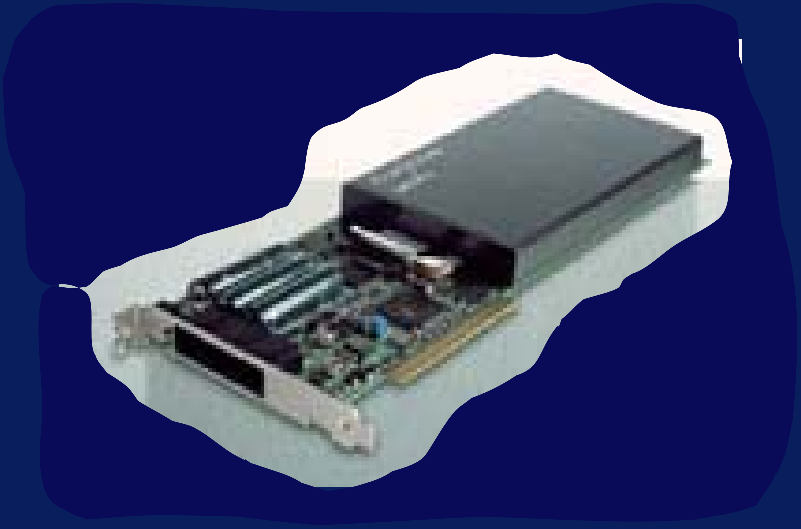
- Dificult to fit in non physical attacks
  - -perturbation
  - -side channel attacks
- Modern chips have protection at all levels
- Criterium is work effort



Multichip standalone crypto modules

Payment terminal or Host Security Module

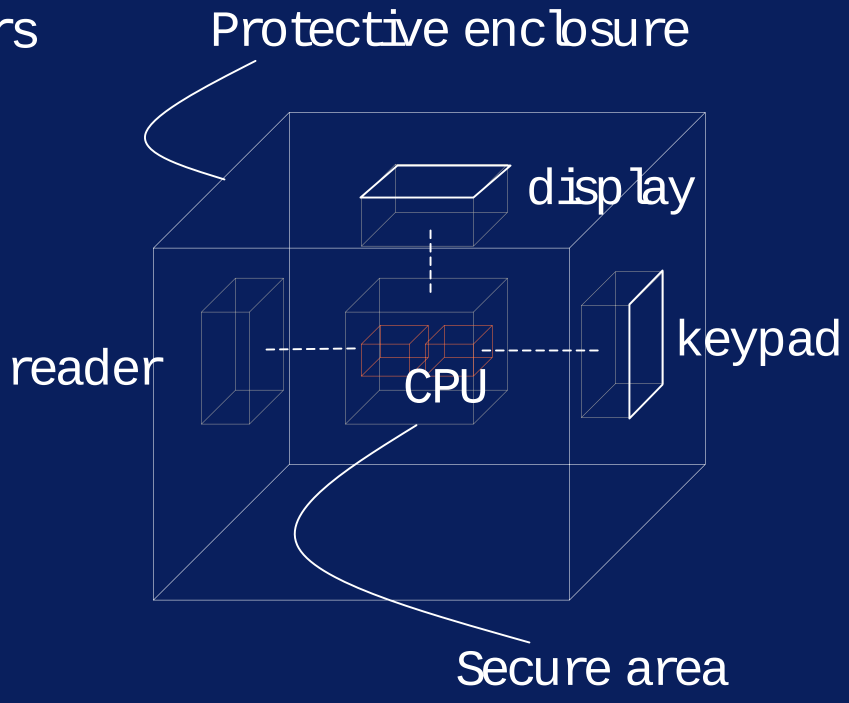




Architecture model

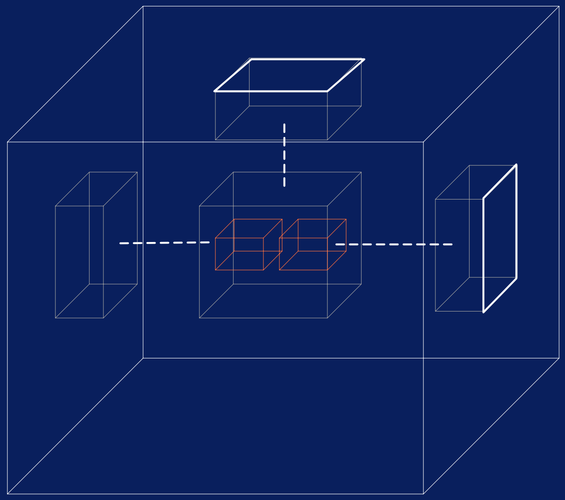
Possible attacks:

- Physical penetration
- Misuse of maintenance covers
- Environmental attacks
- Misuse of device
- Side channel
  - -EMA
  - -SPA/DPA
  - -Noise
  - -cross talk
- Perturbation
  - -Temperature
  - -Radiation
  - -voltage



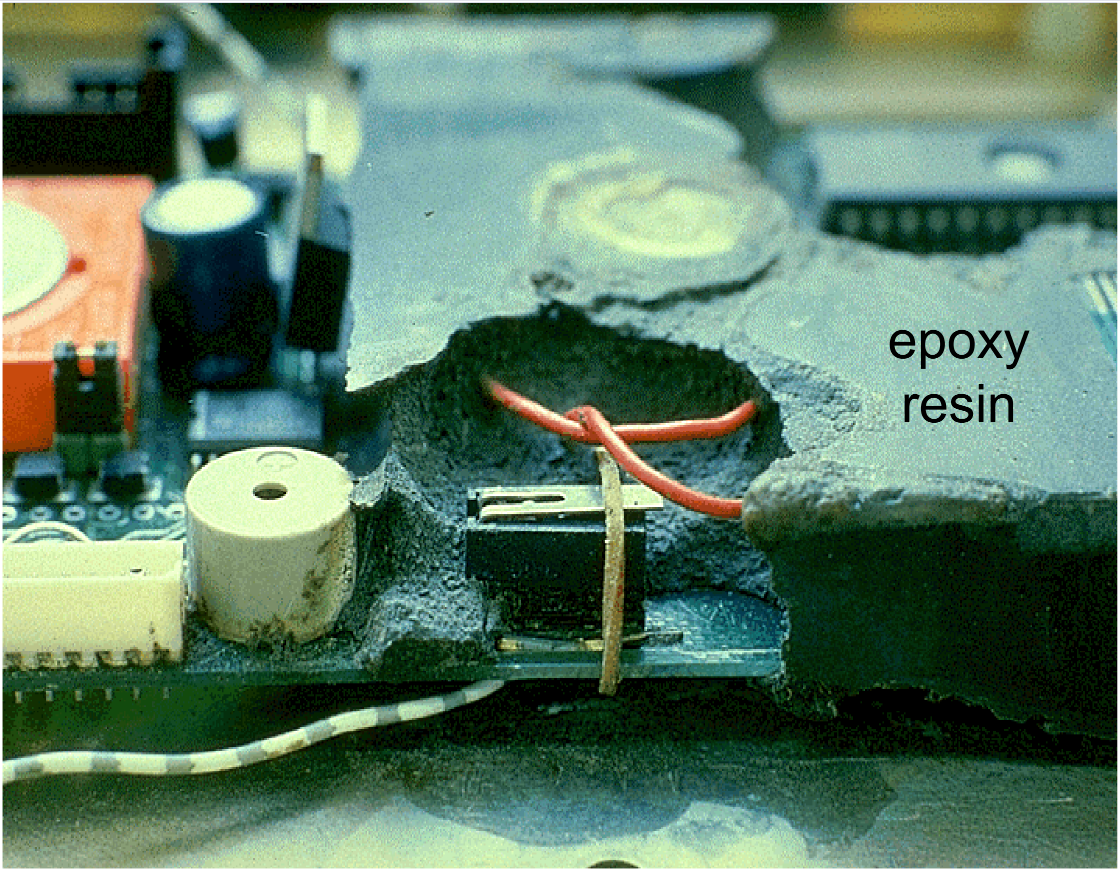
Example security requirements

- Secure enclosure
  - Tamper evidence
  - Tamper resistance
  - Tamper responsive
- Secure area
  - e.g potting
- Switches
- Unique enclosure
- Environmental protection



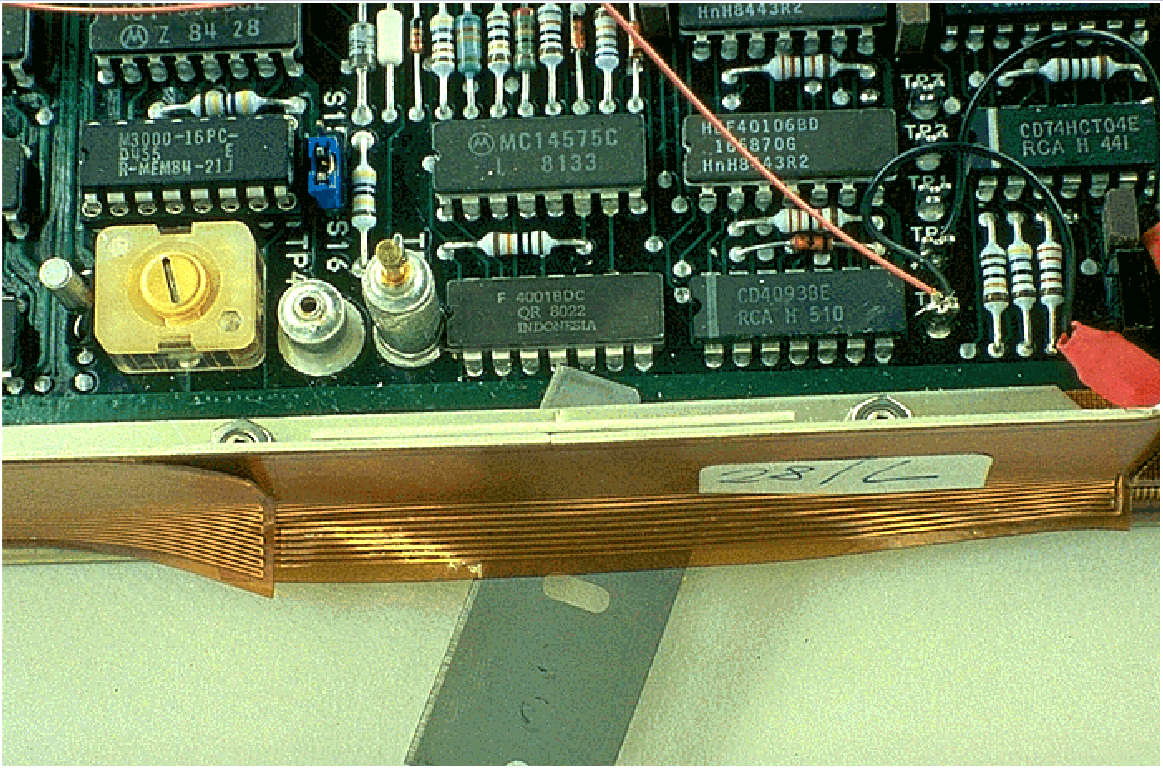
Adequacy of requirements

Requirement for potting and effectiveness of potting



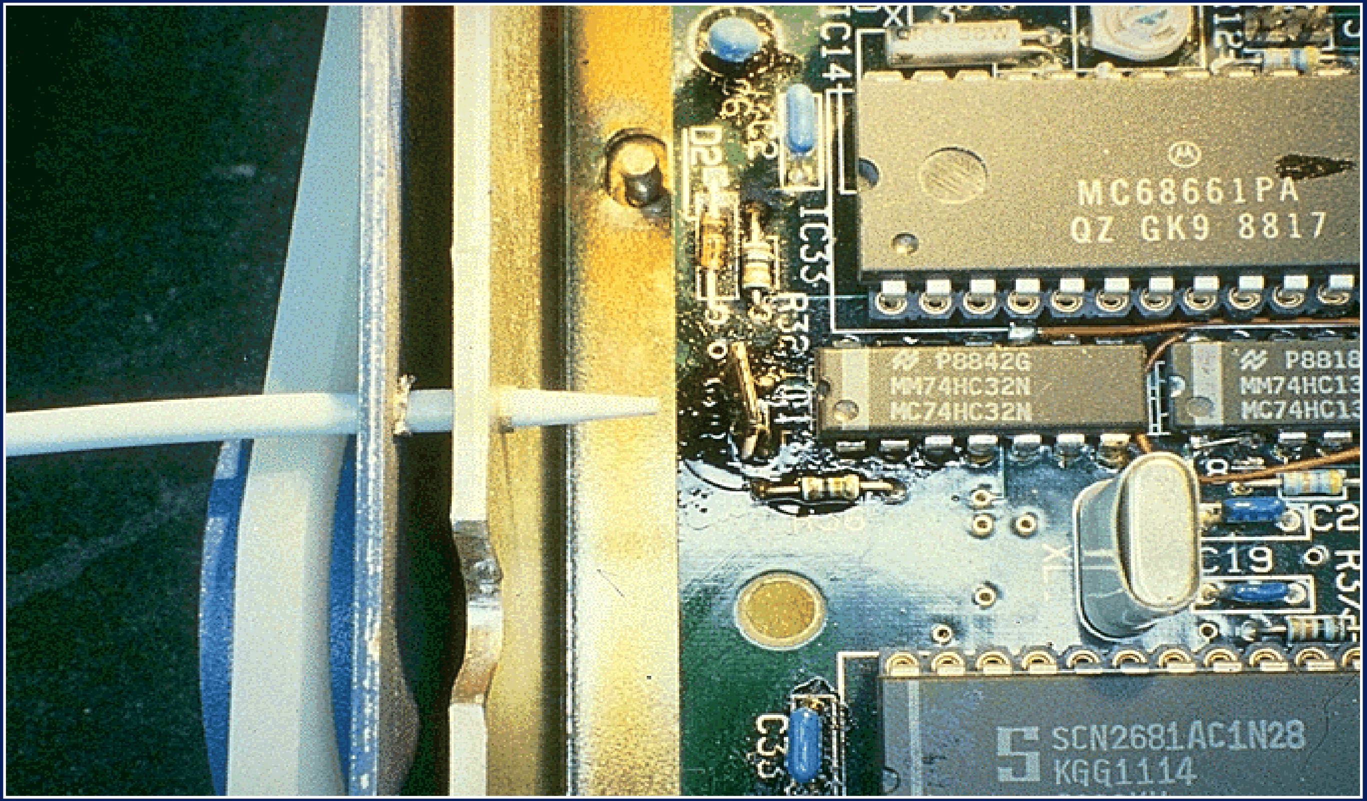
Adequacy of requirement

Requirement for protection against penetration of enclosure preventing holes larger than … .



Adequate security requirements

Light sensor



Problems

- Terminals get internet connections; reference model is incomplete for these options
- Manufacturer has a solution that overcomes the use of potting; product very good but problems to get it accepted;
- Integration of keyboard and display in touchscreen; Reference model is no longer applicable which presents problems on what and how to test;
- Open Platform PDA's provide opportunities but also threats on uniqueness of enclosures

Conflicting interests

- Manufacturers tend to design towards the requirements to minimise costs:
  -clear requirements on what and how to test;
- End users want protection against threats:
  -security is a moving target
- Labs are asked to evaluate security?
  -validate implemented measures
  -evaluate effectiveness?
  -how far to go?

Approaches in security requirements

How to get the best of two extremes?

High level	Technical level
• Long life because independent of technology and design • Facilitates innovation • Lab makes choices for testing • Consensus needed on attacks	• Short life because model becomes inadequate • May hamper innovation • Consistency in testing (box ticking)

Suggestions

- Do not make requirements restrictive
- Address the test goal
- Give some freedom to the lab?