

A FIPS 140-2 evaluation could easily encompass physical security tests

Jean-Pierre KRIMM

CESTI-LETI

jean-pierre.krimm@cea.fr

Physical Security Testing Workshop

26 - 29 September, Honolulu

www-leti.cea.fr

CESTI-LETI Presentation



- **A French ITSEF**
- **Belongs to a public institution (independence)**
- **Accredited for electronic components and embedded softwares**
- **Performs CC and ITSEC evaluations**

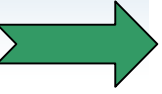
Who I am

- an evaluator (software) in the CESTI-LETI
- involved in ITSEC and Common Criteria evaluations for smart cards
- in charge of various R&D projects (PKI, semi-formal and formal CC evaluation tasks)
- representing CESTI-LETI in several international security working groups (E-europe TB3/SG1, ISCI WG1 on methodology and evaluation criteria)
- involved in FIPS 140-2 evaluation, and ISO/IEC 19790 standard

Context of this presentation

- **My own skills: the Smart Cards' World**
 - **Common Criteria evaluation**
 - ✗ a lot of time spent for physical testing
 - **FIPS 140-2 validation**
 - ✗ mainly conformance tests
- **The Common Criteria and FIPS 140-2 are different**
 - abstractness
 - focus of tests (conformance vs evaluation)
- **What is the area of the intersection of these two worlds?**

Presentation Outline

- 
- **CC evaluation vs FIPS 140-2 validation**
 - general overview

 - **Presentation of some attacks actually performed in CC smart card evaluations**

 - **How the results of these attacks are taken into account in CC evaluation**

 - **How these attacks could be taken into account in FIPS 140-2 validation**

CC Evaluation vs FIPS 140-2 Validation

	CC	FIPS 140-2
Actors	CB Testing Lab.	CMVP, CAVP, NIST/CSE Testing Lab.
Laboratories	ITSEF (CB in each scheme)	CMT Lab (NVLAP)
Prerequisite	None	Crypto algo validation (CAVP)
Product	Target Of Evaluation	Cryptographic Module
Applicability	All	US and Canadian Organization
Description	Security Target	Security Policy
Security Levels	7 EAL, 4 robustness levels	4 Security Levels
Methodology	CEM	DTR
Philosophy	Evaluation	Validation
Tester Tasks	SAR	Security Areas

Security Assurance Requirements (CC)

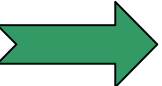
Choose a level in the following Classes

- Security Target Evaluation (ASE)
- Configuration Management (ACM)
- Delivery and Operation (ADO)
- Development (ADV)
- Guidance Documents (AGD)
- Life Cycle Support (ALC)
- Tests (ATE)
- Vulnerability Assessment (AVA)

FIPS 140-2 Security Areas

- Cryptographic Module Specification
- Cryptographic Module Ports and Interfaces
- Roles, Services, and Authentication
- Finite State Model
- Physical Security
- Operational Environment
- Cryptographic Key Management
- EMI/EMC requirements
- Self Tests
- Design Assurance
- Mitigation of Other Attacks

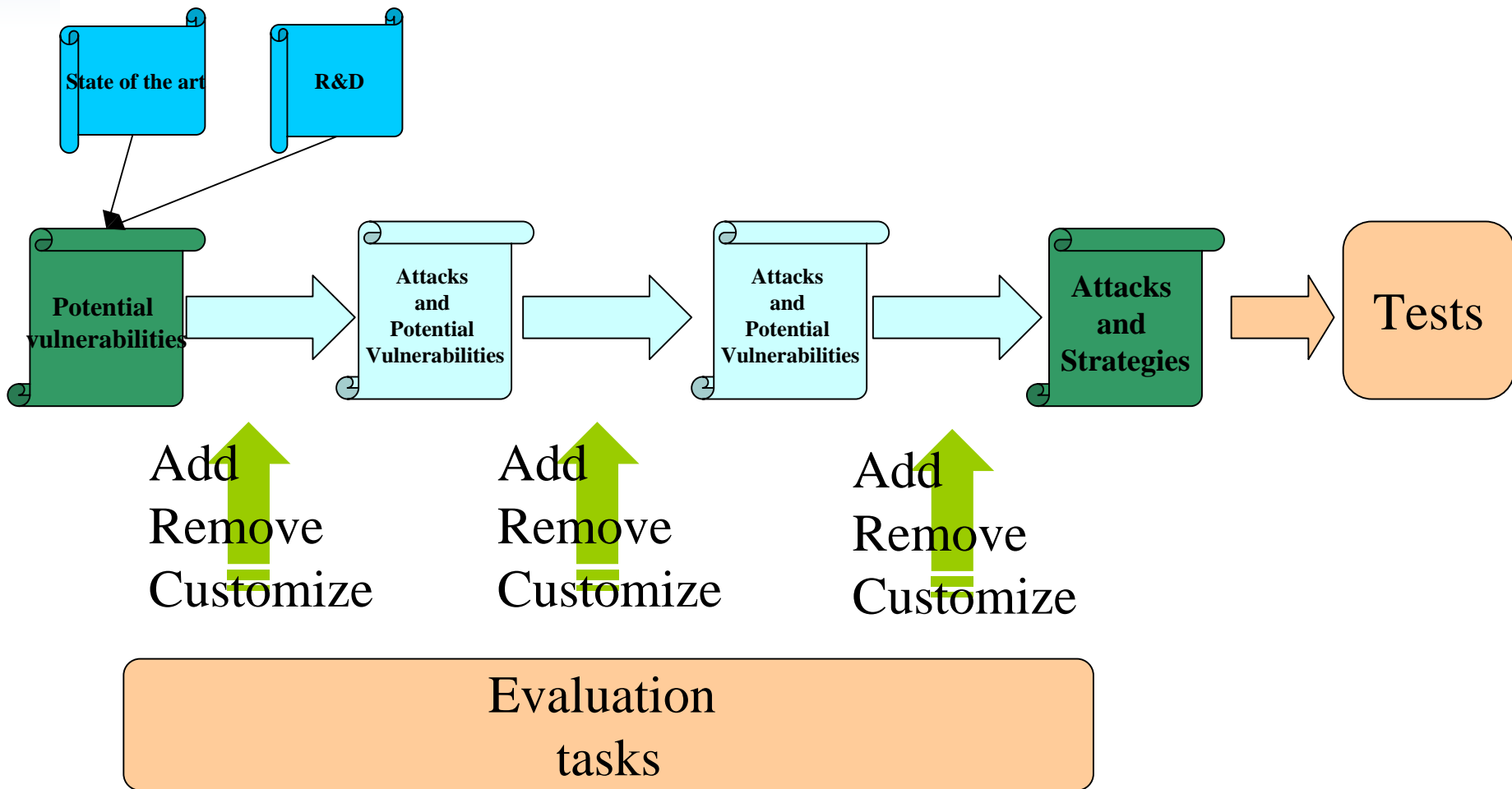
Presentation Outline

- **CC evaluation vs FIPS 140-2 validation**
 - general presentation
-  ■ **Presentation of some attacks actually performed in CC smart card evaluations**
- **How the results of these attacks are taken into account in CC evaluation**
- **How these attacks could be taken into account in FIPS 140-2 validation**

Which tests are performed

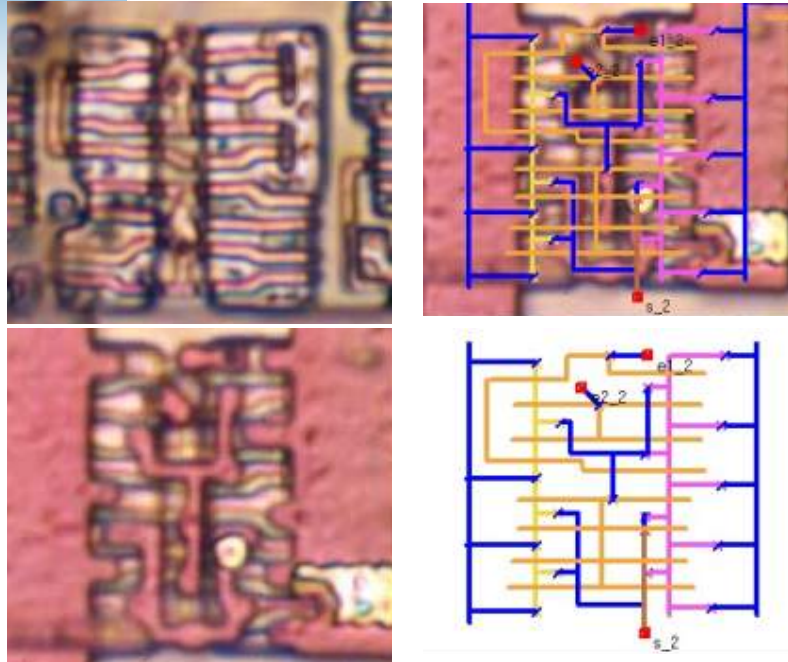
- **Functional testing but security oriented**
 - Are the Security Functions working as specified ?
- **Penetration testing**
 - Independent vulnerability analysis
 - Adaptation of the classical “attack methods” to the specificities of the product

Strategy for penetration testing



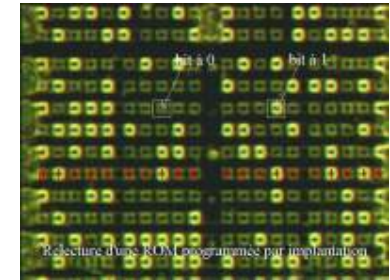
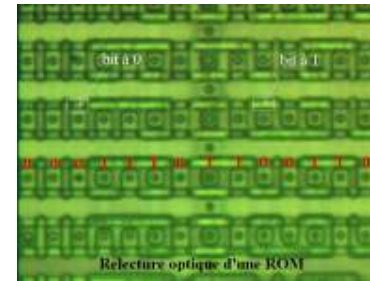
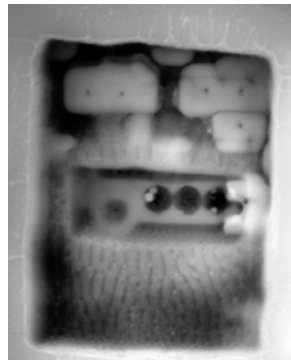
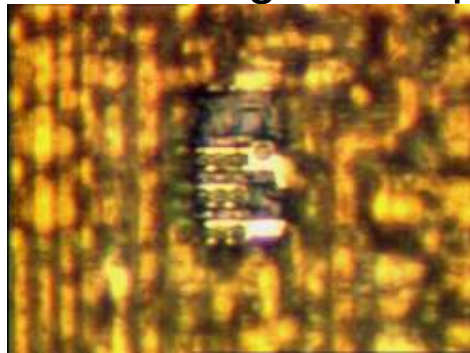
Attacks on Smart Cards

- **Physical (Silicon related)**
 - Memories
 - Access to internal signals (probing)
- **Side Channel Analysis**
 - SPA, EMA, DPA, DEMA
- **Perturbations**
 - Cryptography (DFA)
 - Generating errors
- **Specifications/implementation related attacks**
 - Protocol, overflows, errors in programming, ...



Reverse Engineering

Probing : laser preparation



Optical reading of ROM

Probing : MEB

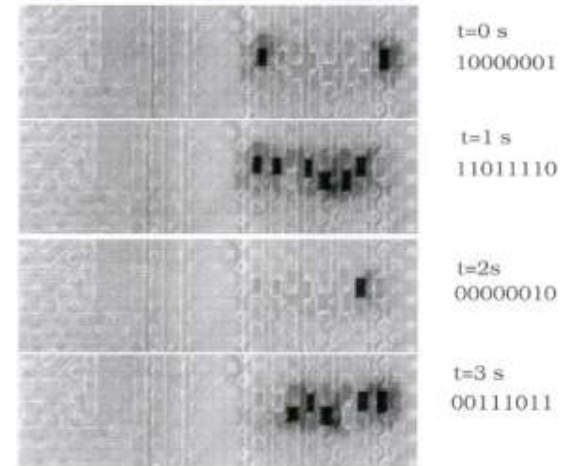
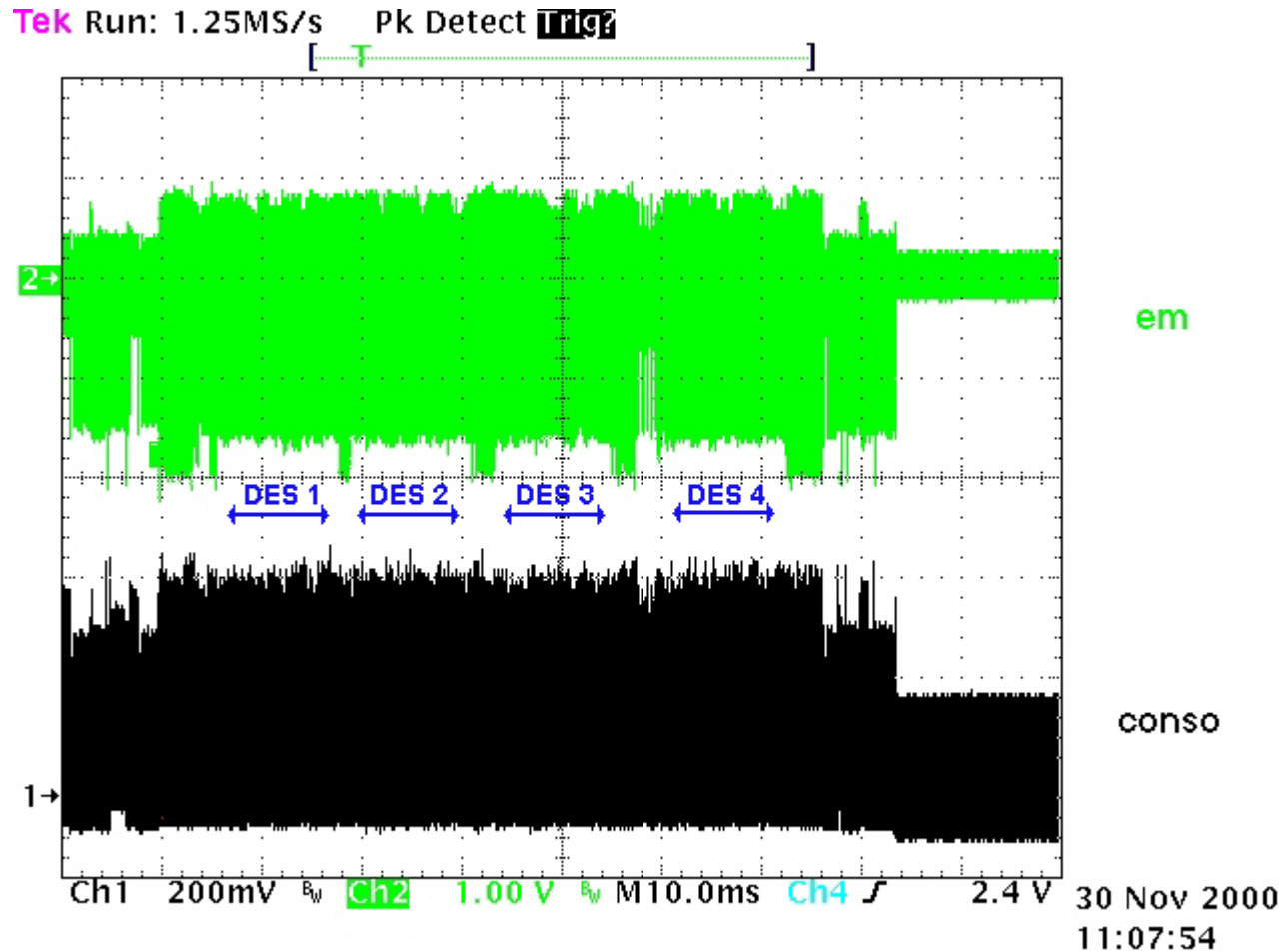


Figure 2: Image sous faisceau d'électrons en contraste de potentiel des états électriques des lignes du bus de données en fonction du temps.

EM Signal Analysis

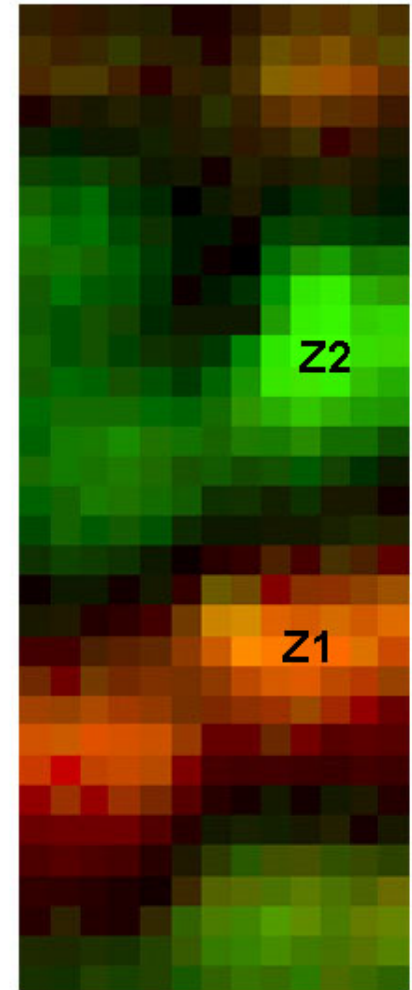


Electro-magnetic signal during
DES execution.

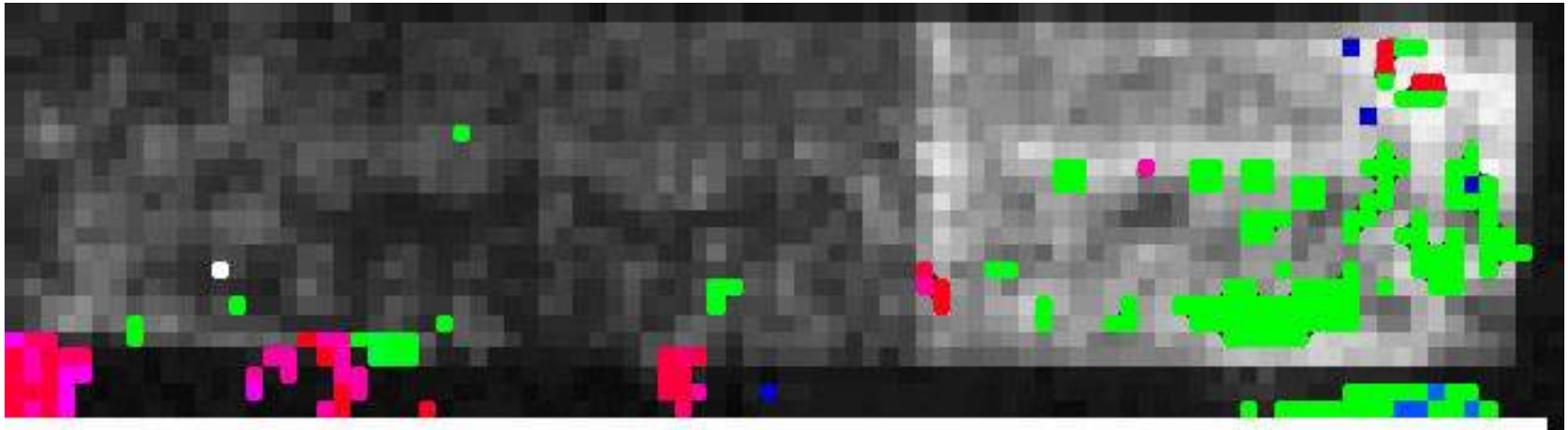
- Hardware DES
- Differential signal



Signal amplitude



Signal difference



- DES errors
- Device restart

Light perturbation of Hardware DES

Perturbations Examples

Initializations

valid = TRUE;

**If got \neq expected then
valid = FALSE ;**

If valid Then
critical processing;

Branch on error

Non critical processing;

If not authorized then goto xxx;

Critical processing;

Re-reading after integrity checking

Memory integrity checking;

Non critical processing;

Data 1 reading;

Critical processing;

Data 2 reading;

Critical processing;

What is requested for the ITSEF

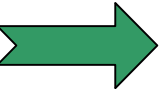
- **Good knowledge of the state of the art**
 - Not always published
- **Internal R&D on attacks**
 - Equipment
 - Competences
- **Multi-competences**
 - Cryptography, microelectronics, signal processing, lasers, software, ...
- **Competence areas defined in the French Scheme**
 - Hardware (IC, IC with embedded software)
 - Software (Networks, OS, ...)

Summary of attacks in CC evaluations

- **CC Evaluation is**
 - Rigorous & normalized process
 - Gives the assurance that the product is as resistant as it is declared in the ST
 - Attacks also need specific « human » skills

- **Attack is**
 - Gaining access to secret/forbidden operations
 - Free to « play » with the abnormal conditions
 - An error is not an attack
 - ✘ But an error can often be used in attacks

Presentation Outline

- **CC evaluation vs FIPS 140-2 validation**
 - general presentation
- **Presentation of some attacks actually performed in CC smart card evaluations**
-  ■ **How the results of these attacks are taken into account in CC evaluation**
- **How these attacks could be taken into account in FIPS 140-2 validation**

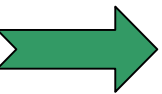
A Quotation Table Exists (JIL)

Factors	Identification	Exploitation
Elapsed time		
< one hour	0	0
< one day	1	3
< one week	2	4
< one month	3	6
> one month	5	8
Not practical	*	*
Expertise		
Layman	0	0
Proficient	2	2
Expert	5	4
Knowledge of the TOE		
Public	0	0
Restricted	2	2
Sensitive	4	3
Critical	6	5
Access to TOE		
< 10 samples	0	0
< 100 samples	2	4
> 100 samples	3	6
Not practical	*	*
Equipment		
None	0	0
Standard	1	2
Specialized	3	4
Bespoke	5	6

Range of values	Resistance to attacker with attack potential of:	SOF rating
0-15	No rating	No rating
16-24	Low	Basic
25-30	Moderate	Medium
31 and above	High	High

Presentation Outline

- **CC evaluation vs FIPS 140-2 validation**
 - general presentation
- **Presentation of some attacks actually performed in CC smart card evaluations**
- **How the results of these attacks are taken into account in CC evaluation**
- **How these attacks could be taken into account in FIPS 140-2 validation**



Possible interpretations

- **a DTR statement is incomplete**
 - "Attempt to access (by circumventing the documented protection mechanisms) [...]"
 - in tester requirements TE03.22.02 (RSA) and TE07.01.02 (CKM)

- **2 interpretations are possible**
 - Using Only External Interfaces of the Module (Functional Means)
 - Or going further: Performing Environmental and/or Physical Testing

- **Identified Problems**
 - How to quote the attacks ?
 - How to know if the attack leads to a fail verdict ?
 - Which quotation for each security level ?
 - How modified the NVLAP taking into account the attacks skills ?

- **Proposals**
 - Using the CC Smart Card Quotation Table
 - VLA.1 for level 3 and VLA.2 for level 4 (can be augmented)

A Feasibility Study

- **Outside FIPS Applicability Context**
 - EMI/EMC does not apply
 - "FIPS Approved" has been re-defined
- **Performed by the CESTI-LETI
Q4 2004 - Q1 2005**
- **Sponsored by the DCSSI**
- **The Cryptographic Module was already certified**
- **Two Phases in this project**
 - FIPS 140-2 evaluation (adapted security areas)
 - Capitalization reports
(general, methodology and process)

- **The DCSSI is involved in ISO/19790 standard**
- **The Context of the Feasibility Study Applies**
- **Methodology Report of the Feasibility Study has been used as input**
- **The Physical Security Testing could be considered, but how ?**

- **CC evaluation and FIPS 140-2 validation are different but:**
 - We can introduce vulnerability assessment on Cryptographic Modules
 - We can use the same Quotation Table as for CC
 - This can lead to a common scheme for the penetration testing allowing some comparisons

- **The penetration testing is not "self-acting" in CC evaluations**

Thank you for your attention



Jean-Pierre Krimm

jean-pierre.krimm@cea.fr
