Trifón Giménez
Epoche & Espri
eval@epoche.es

EPOCHE & ESPRI

Side Channel Analysis

Scoring attack potential under AVA_VAN.5

Common Criteria

Agenda

EPOCHE & ESPRI

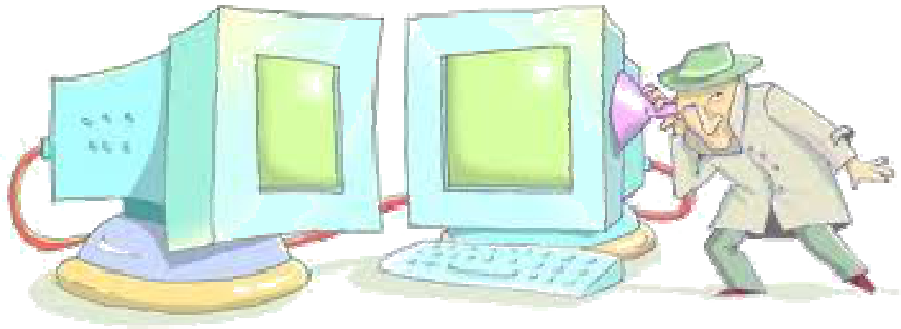
- Introduction to SCA
- Current Situation
- Proposal
- Scoring Attack Potential
- Conclusions

Introduction

EPOCHE & ESPRI

- Side Channels leaking
  - Timming, Power Consumption, Emanations…
- Consumptions depends on Operations
- Statistical Analysis

  Hypothesis vs. Consumption



Power Consumption & Electromagnetic Emanation

Current Situation

EPOCHE & ESPRI

- CC
  - Excludes evaluation of some hardware aspects

- JIL Smart-Cards
  - AVA_VAN.5

- Other Initiatives
  - ISO 17825 (Working Draft)
  - FIPS 140-3

Embracing HW evaluation

EPOCHE & ESPRI

- CC
  - Explicit assurance evaluation activities associated to functional requirements
    - New vision PPs
    - See "An XML extension of the CC/CEM to cover the new CPP“ by Miguel Bañón
    - See the evaluation methodologies for Smart Cards
  - Rephrase the CC to embrace HW evaluations
    - Different characteristics but common techniques
    - Compatible with the existing VA and attack potential ratings

Proposal

- Motivation

SCA in AVA_VAN 3 & 4

- Parameters
  - Environment
  - Measurement
  - Analysis

Environment

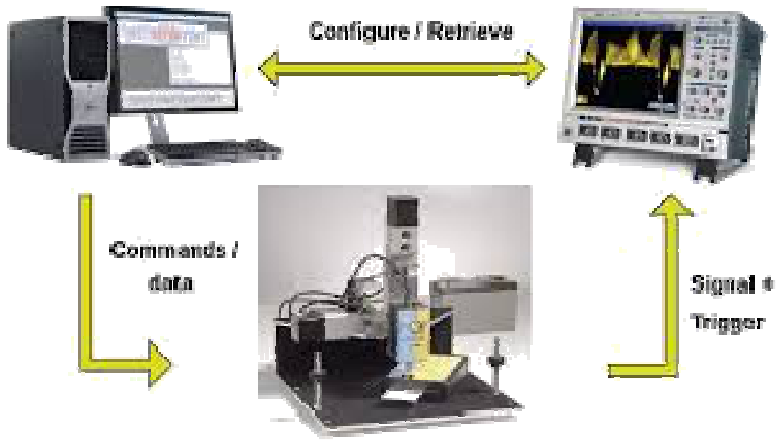
- Accessible TOE?
  - Trigger
  - Measurement Point

Mandatory?

Security Boxes

- TOE configuration & operation
  - Instrumentation

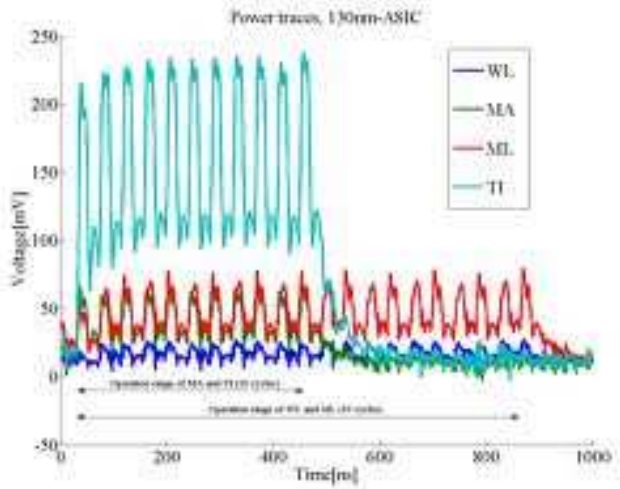
- Oscilloscope
  - Frequency (2 x TOE)



Measurement

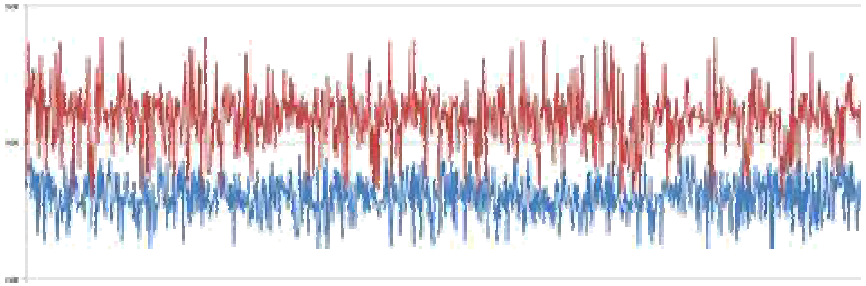
- Appropriate Signal?
  - Amplifiers, Filters
- # of Traces
  - TOE dependency
  - ↑ traces ➔ ↑ time
- Quality

  + resolution ➔ better analysis ☺ ➔ bespoke tool ☹



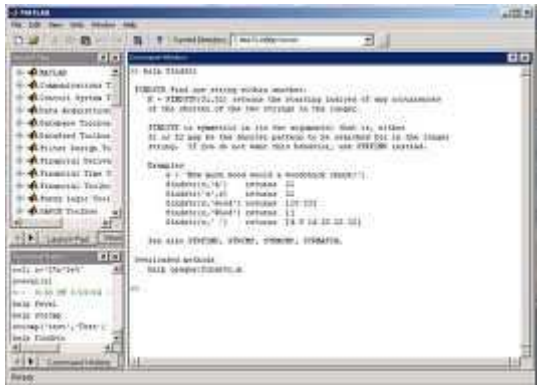
Analysis

- Signal Processing
  - Leakage
    - Countermeasures
  - Noise Reduction?
    - Average Calculation
    - Frequency filters
  - Misalignment?



Attack

- SPA, DPA, CPA, 2º order attacks, …
- Parameters
  - Power consumption hypothesis
  - Statistic Test applied
- Success?
  - Criterion / Decision Factor



Scoring Attack Potential

EPOCHE & ESPRI

Measurement Environment	
PCI board	**Router**
[1 – 3 days] ❑Physically Accessible ❑Measurement Point ❑Trigger ❑Low/Medium Oscilloscope Specialized $	[3 – 5 days] ❑Physically Protected ❑Security Boxes Application ❑Medium/High Oscilloscope $$$ ~ Bespoke

Scoring Attack Potential

EPOCHE & ESPRI

Measurement	
PCI board	**Router**
[1 - 3 days] ❑Simple TOE Operation ❑Signal OK ❑No amplifiers ❑1.000 points per trace	[3 – 7 days] ❑Homemade TOE Operation ❑Signal Weak ❑ Tailored Amplification ❑100.000 points per trace

Layman

Expert

Scoring Attack Potential

EPOCHE & ESPRI

Analysis: Signal Pre-processing	
PCI board	**Router**
[1 - 2 days] ❑Noise? ❑Average noise reduction Layman	❑Countermeasures? [3 – 5 days] ❑Noise? ❑Average noise reduction ❑Frequency filters Bespoke Expert ❑Misalignment? ❑Static Alignment

Scoring Attack Potential

EPOCHE & ESPRI

Analysis: Attack	
PCI board	**Router**
❑Known Attacks ❑SPA, DPA, DEMA *[1 – 3 days]* ❑Result ❑Correlation / Leakage or ❑Key Extraction **Proficient**	❑Bespoke Attacks *[3 – 10 days]* ❑Tailored Consumption / Emantion Hypothesis ❑Adapted Statistic Test ❑SPA,DPA/DEMA, 2º Order **Bespoke** ❑Result ❑Key Extraction **Expert**

Scoring Attack Potential

EPOCHE & ESPRI

AVA_VAN.3		Factor	AVA_VAN.4	
<= two weeks	2	**Elapsed time**	<= one month	4
Proficient	3	**Expertise**	Expert	6
Public	0	**Knowledge of TOE**	Public	0
Easy	1	**Window of opportunity**	Easy	1
Specialized	4	**Equipment**	Bespoke	7
	10	**TOTAL**		18

Enhanced Basic **Moderate**

Conclusions

EPOCHE & ESPRI

- Side channel may be commensurate with AVA_VAN.3 & 4 attack potentials
- Critical factors for applicability
  - Adequate TOE
  - Measurement
  - Analysis
- SCA on evaluations NOW
  - CC Products may be leaking at this time!!

Trifón Giménez
eval@epoche.es

Epoche & Espri, S.L.
Avda. de la Vega, 1
28108, Alcobendas, Madrid
Spain

Tel: +34 914-902-900
FAX: +34 916-625-344

Epoche & Espri Corporation
4000 Legato Road, Suite 1100
Fairfax, VA 22033
USA

Tel: +1 888-877-9506
FAX: +1 703-227-7189