Testing Fault Injection and Side Channel in FIPS

Vision of a Smart Card Laboratory

José Francisco Ruiz Gualda
& David Hernández
IT Area
Applus+ Laboratories

Agenda

- 01. Introduction
- 02. Security threats
- 03. Side Channels attacks
- 04. Fault Injections attacks
- 05. Applus+ Solutions

Introduction

Who are We?

José Francisco Ruiz

- Graduate in computer science with more than 8 years' experience in IT security under CC and FIPS 140-2 standard
- **Manager of the Common Criteria** service in Applus+ Laboratories
- Participating in more than 40 security evaluations from EAL1 to EAL5 (Smart Cards, Security boxes, software, hardware, etc...)
- Talks in several ICCC conference

David Hernández

- PhD in Electronic Engineering
- +5 years' experience in security evaluations under EMVCo and CC standards
- **R&D Manager** for projects in the field of SCA and Crypto
- In charge of the technical training for new employees

Introduction

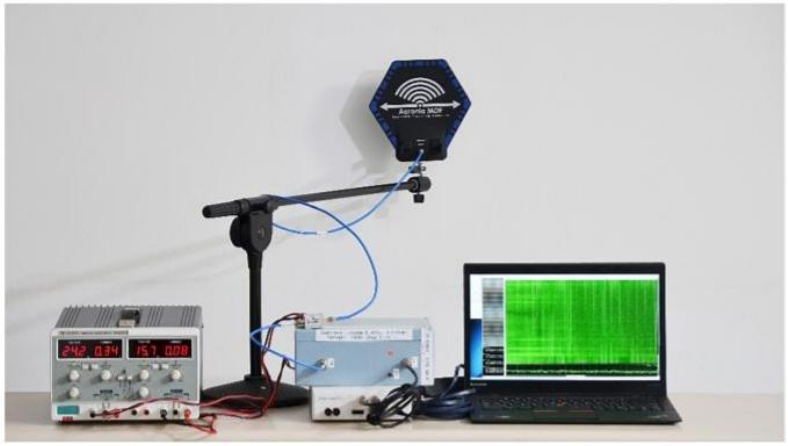
About Applus+ Laboratories (Why are We here?)

- Applus is involved in many evaluations schemes (Common Criteria, EMVCo, GlobalPlatform, VISA, Mastercard, etc.). In this way, we can pulse the different security schemes evolution, following the market needs
- Several team members have Background in FIPS 140-2.
- Applus wants to share its vision of the threats that are applicable for Cryptographic modules and are not being considered in FIPS 140-2.

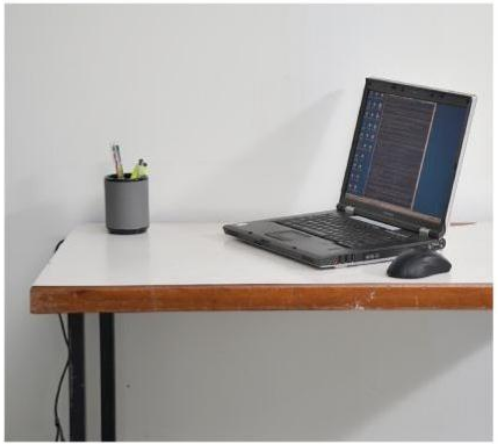
Are FIPS 140-2 requirements enough to ensure the robustness of Cryptographic Modules?

Security Threats

Stole Crypto Keys from an Offline Laptop in Another Room (February 16, 2016)



(a) Attacker's setup for capturing EM emanations. Left to right: power supply, antenna on a stand, amplifiers, software defined radio (white box), analysis computer.



(b) Target (Lenovo 3000 N200), performing ECDH decryption operations, on the other side of the wall.

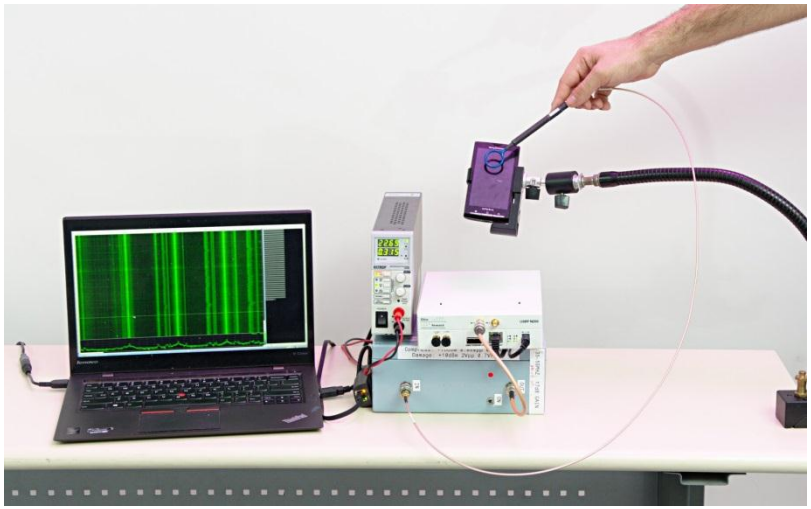
Figure 6: Attacking a target computer in an adjacent room, across a wall.

$3000 attack againts GnuPG ECDH implementation

Paper: https://eprint.iacr.org/2016/129.pdf
Press article: http://motherboard.vice.com/read/how-white-hat-hackers-stole-crypto-keys-from-an-offline-laptop-in-another-room

Security Threats

Side-Channel Attack Steals Encryption Keys from Android and iOS Devices (March 15, 2016)

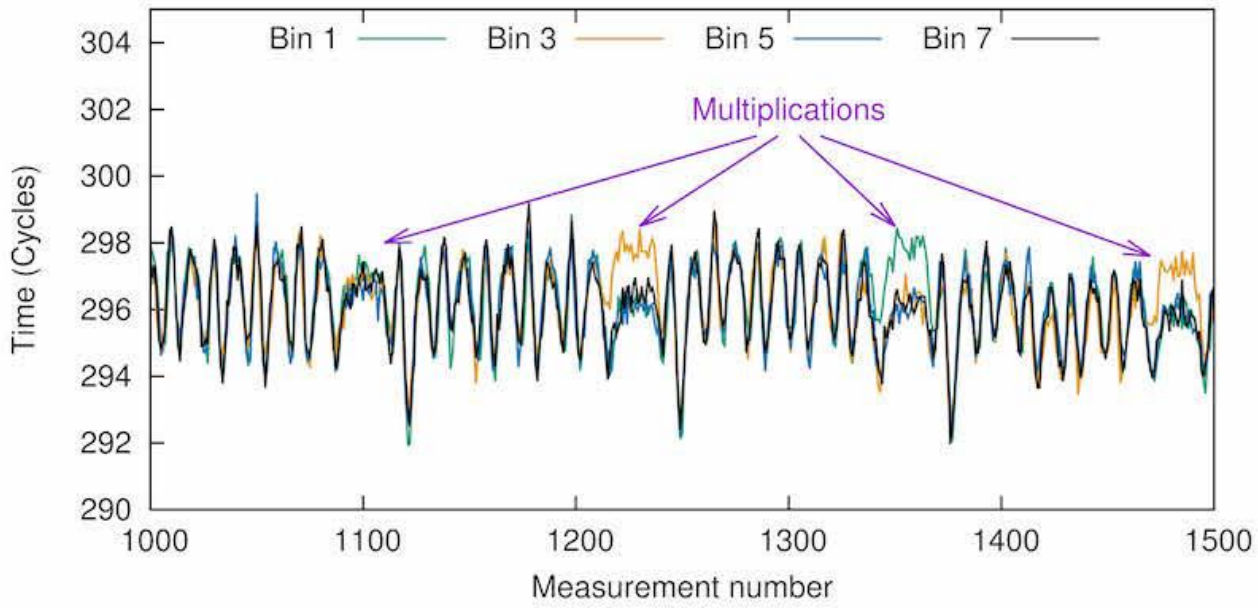


Attack againts ECDSA on OpenSSL and CoreBitcoin.

Paper: https://www.cs.tau.ac.il/~tromer/mobilesc/mobilesc.pdf
Press Article: http://news.softpedia.com/news/new-side-channel-attack-steals-encryption-keys-from-android-and-ios-devices-501373.shtml

Security Threats

CacheBleed OpenSSL Vulnerability, Intel CPUs are affected (March 2, 2016)



Attack gets recover RSA 2048-bit and 4096-bit secret keys.

First cache-bank side-channel attack

Paper: http://ssrg.nicta.com.au/projects/TS/cachebleed/cachebleed.pdf

Press Article: http://news.softpedia.com/news/cachebleed-openssl-vulnerability-affects-intel-based-cloud-servers-501229.shtml

Which testing requirements should be included in new versions of CMVP program?

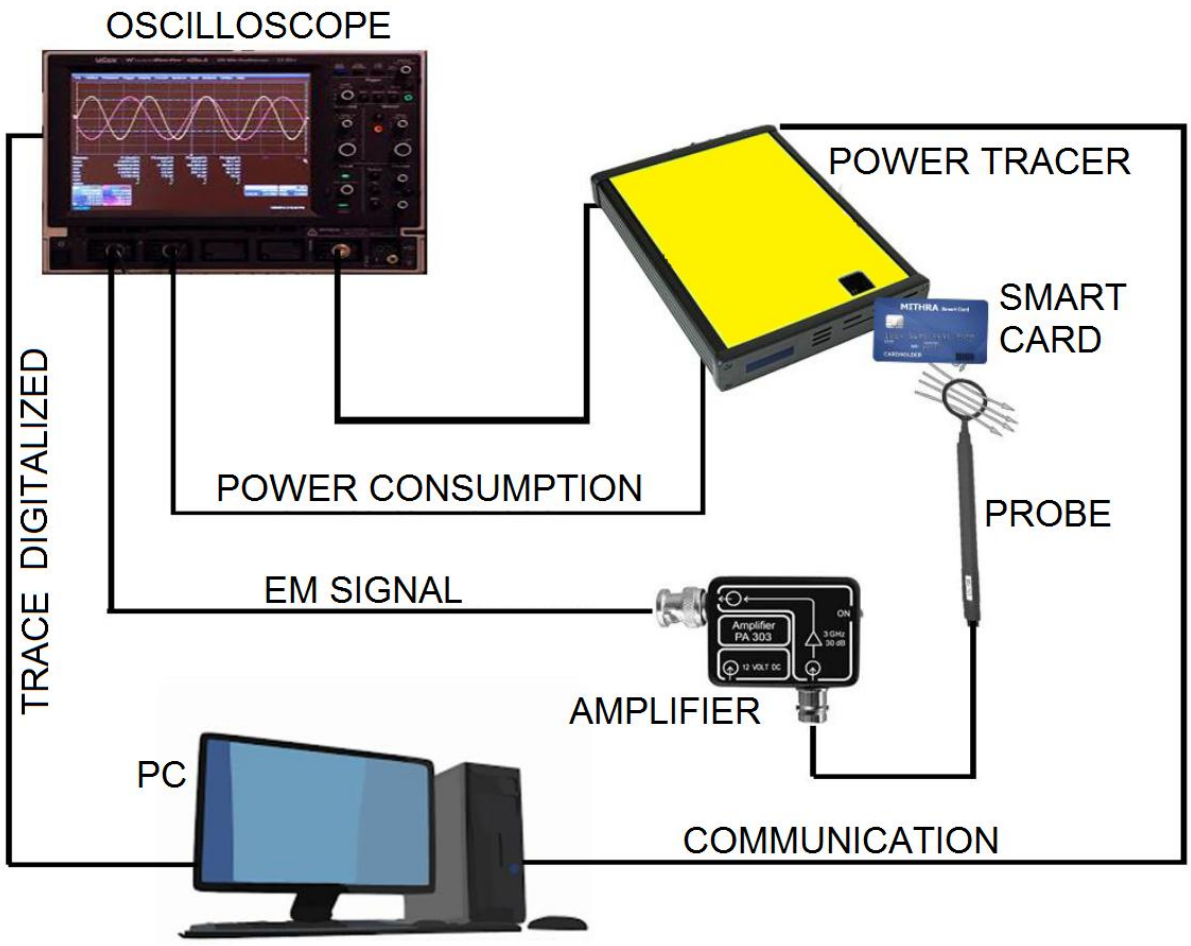
Side Channel Attacks

What are Side Channel Attacks?

- A side channel is an unintended communication channel leaking information through a physical media (e.g. power consumption, electromagnetic radiation, photonic emission)
- An attacker exploits the information leaked to recover secret data from the TOE
- Generally speaking, side channel cannot be avoided, i.e. countermeasures do not actually make attacks infeasible, however they are expected to increase attackers' experimental and computational workload (data acquisition and processing) beyond reasonable limits

Side Channel Attacks

Testing Set up

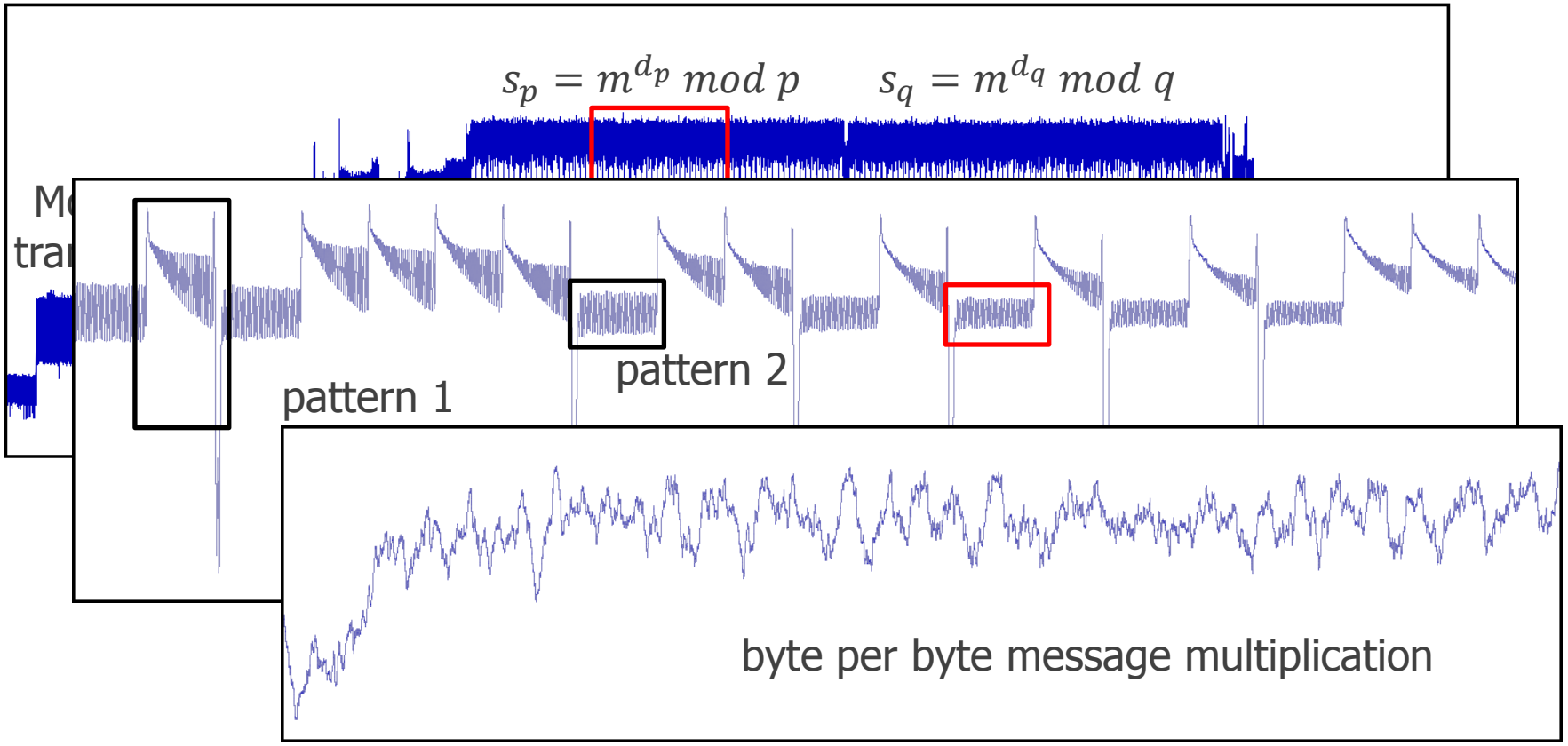


Test campaign costs:

- ✓ 2-30k oscilloscope
- ✓ 6-20k EM set-up
- ✓ 1-6k PC with SCA tool

Side Channel Attacks

Example: **Electromagnetic radiation of RSA-CRT**



Side Channel Attacks

Applus+ Side Channel evaluations:

- **TOEs:** smart cards (credit cards, ID-cards, e-passports), cell phones (white box crypto, TEE), chips, secure flash

- **Methodology:** two scenarios,
  - ✓ *white box evaluation*, complete review and total access to TOE, vulnerability analysis and attack path
  - ✓ *black box evaluation*, test vector leakage assessment (TVLA)

- **Attacks:** SPA/SEMA, DPA/DEMA, Sliding Window DPA, CPA/CEMA, Address bit DPA, Horizontal Power Analysis, HO attacks, Template Attacks…

Fault Injection Attacks

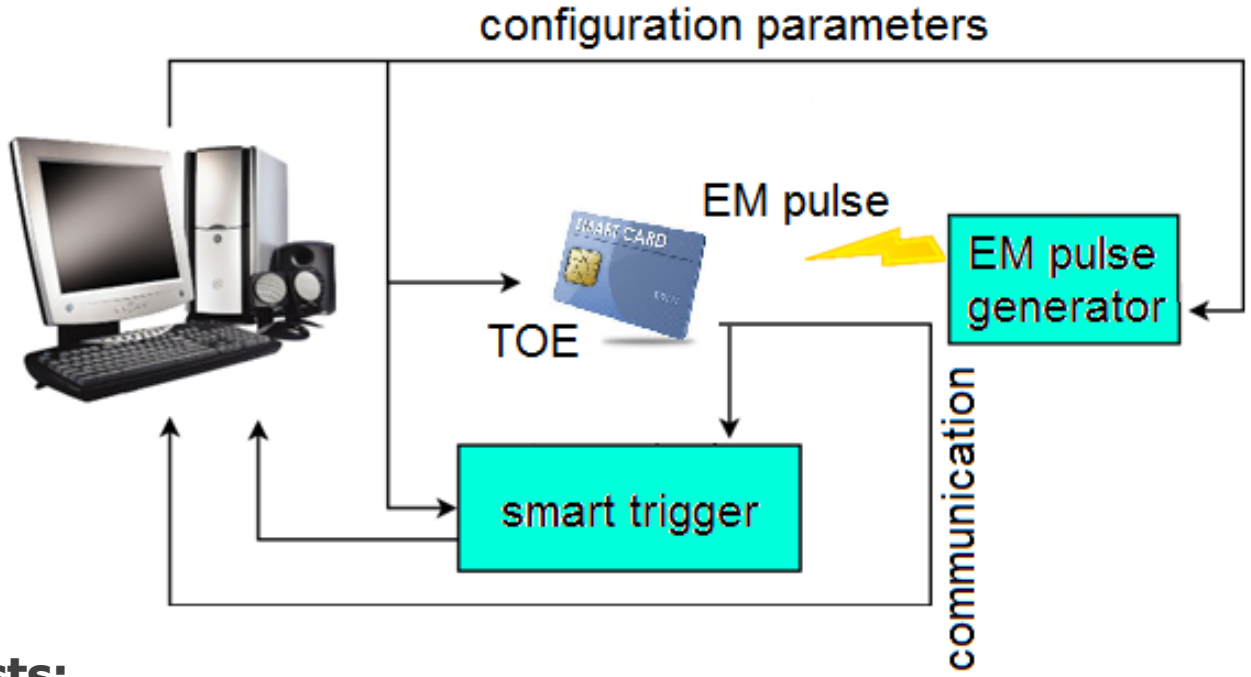
What are Fault Injection Attacks?

- Fault injection are semi-invasive attacks in which the TOE is perturbed such a way that security-relevant instructions are altered from their normal behavior
- Fault models:
  - ✓ Skip an instruction
  - ✓ Change the return value of a function
  - ✓ Change the value of data stored in memory / internal registers
  - ✓ Modify data while being processed by the device

Fault Injection Attacks

Applus laboratories

Testing Set up



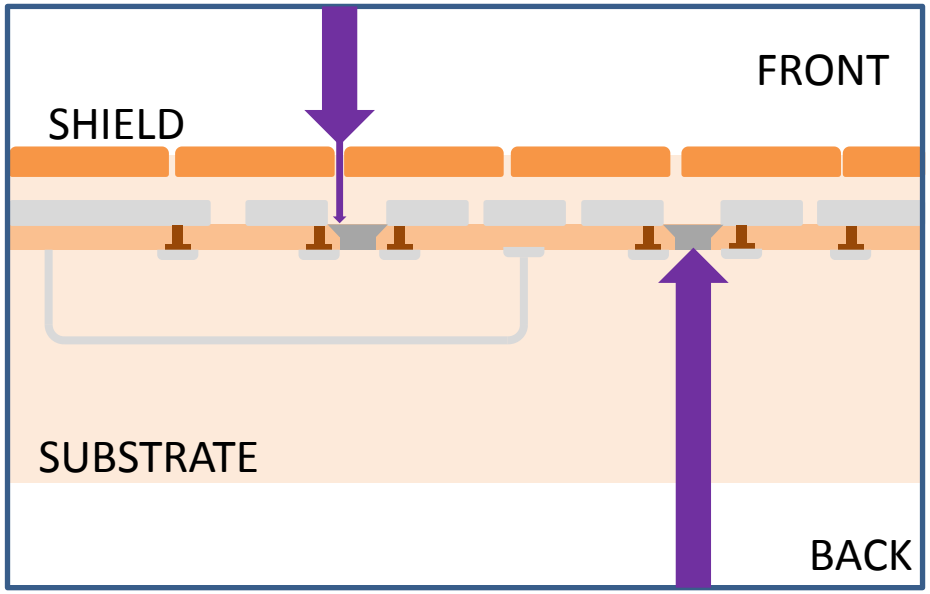
Test campaign costs:

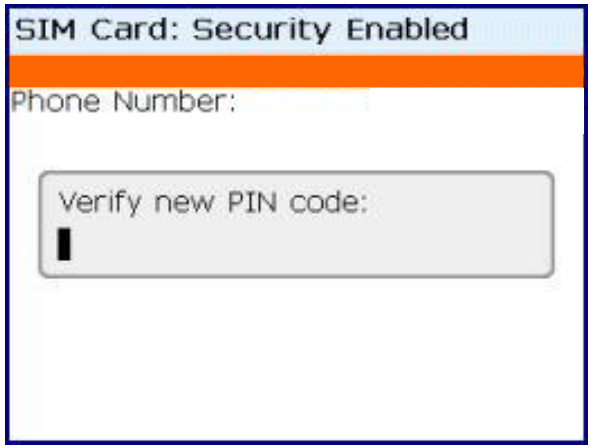
- ✓ 2-30k oscilloscope
- ✓ 10k-40k EM pulse generator (different waveforms)
- ✓ 2k EMI probe and XYZ positioner
- ✓ 10-25k smart trigger
- ✓ 1-6k PC with FI tool

Fault Injection Attacks

Example: **Skipping PIN verification**

- Injecting energy at transistor level to perturb the normal behavior of the TOE and skip an instruction.





Fault Injection Attacks

Applus+ Fault Injection evaluations:

- **TOEs:** smart cards (credit cards, ID-cards, e-passports), cell phones (white box crypto, TEE), chips, secure flash
- **Methodology:** initial side channel analysis with two possible outputs,
  - ✓ operation not possible to localize – fault injection not considered
  - ✓ operation localized in execution time and hardware module affected – attack path defined
- **Attacks:** light injection, EMI, voltage / clock glitching

How to include these requirements to improve Cryptographic Modules Robustness in a cost effective manner?

Applus+ solution

Testing Side Channel in FIPS:

- ISO/IEC 17825:2016 specifies the non-invasive attack mitigation test metrics for determining conformance to the requirements specified in ISO/IEC 19790 for Security Levels 3 and 4
- Applus fully agrees with the specified methodology and test metrics described, and proposes:

Security Level	Workload	Objectives
3	1 week	- Evaluate TOE's resistance against SPA/SEMA and identify timing problems - TVLA to test device's leakage (1st order)
4	3 weeks	- Evaluate TOE's resistance against SPA/SEMA and identify timing problems - TVLA to test device's leakage (1st order) - TVLA to test device's leakage (high order)

Applus+ solution

Testing Side Channel in FIPS:

- The lab is able and has the experience to conduct the described analyses and proposes also **high order resistance assessment** in products with Security Level 4
- More complex attacks such as Template Attacks upon customers' request

Applus+ solution

Testing Fault Injection in FIPS:

- A short characterization campaign is proposed to test TOE's resistance against electromagnetic pulse injection (EMI) and **power line glitch**
- PASS/FAIL result whether the test is able to retrieve the algorithm's secret key or not

Security Level	Workload	Objectives
3	-	- No fault injection assessment proposed
4	1 weeks	- Test strenght of countermeasures against DFA - Retrieve algorithm's secret key

Conclusions

- Resistance against Side Channel attacks must be tested in Cryptographic Modules.
- ISO/IEC 17825:2016 testing approach for side channel is appropriate. However, High Order DPA attacks should be included.
- Resistance against Fault Injection attacks (at least for Level4 IUTs) should be required (at least as an optional item in CMVP validation).
- Smart Cards Labs Experience should be taken into account to face the challenge of Side Channel and Fault Injection Attacks.

THANK YOU VERY MUCH FOR YOUR ATTENTION.

For more information, please contact

Contact details:

José Ruiz Gualda
Common Criteria Leader
jose.ruiz.gualda@applus.com

David Hernández
R&D Manager
david.hernandez.g@applus.com

Applus+ Laboratories
Campus UAB P.O Box, 18
E- 08193 Bellaterra (SPAIN)
M: +34 667 178 009
T: +34 93 567 20 00
F: +34 93 567 20 01