

**10ICCC – Tromso,
Norway**

Spanish Certification Body

**“Walking by the Physical Borderline:
Vulnerability Analysis of HW TOEs with
Security Boxes”**



Dr. Marino Tapiador

September 2009

“Walking by the Physical Borderline: Vulnerability Analysis of HW TOEs with Security Boxes”



Dr. Marino Tapiador

September 2009

Presentation

CONFERENCE: 10th ICCS in Tromso, 2009.

SPEECH: “Walking by the Physical Borderline: Vulnerability Analysis of HW TOEs with Security Boxes”.

GOAL: to present a review of the status-of-the-art in vulnerability analysis and attack methods related to the evaluation of HW TOEs with “security boxes” and how to use this in IT security evaluation methodologies like CC/CEM.

SPEAKER:

Dr. Marino Tapiador. Technical Manager of the Spanish CB.

Centro Criptológico Nacional (CCN)

DATE: September 2009.

Contents

The Physical Borderline

“Security Boxes”

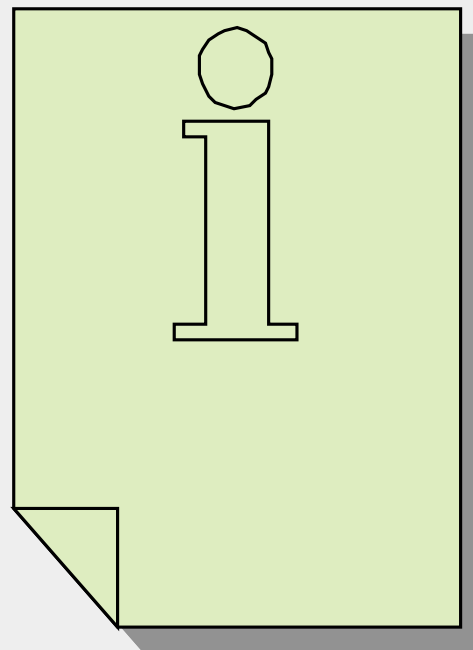
Sec-Box counter-measures

Non-destructive evaluation methods

Destructive evaluation methods

Method for Vulnerability Analysis

Conclusions



The Physical Borderline

CC Part 1

“Certain topics, because they involve specialized techniques or because they are somewhat peripheral to IT security, are considered to be outside the scope of the CC. Some of these are identified below:”

...

CC v2.3: b) “The evaluation of technical physical aspects of IT security such as electromagnetic emanation control is not specifically covered, although many of the concepts addressed will be applicable to that area. In particular, the CC addresses some aspects of physical protection of the TOE.”

CC v3.1: b) “The evaluation of some technical physical aspects of IT security such as electromagnetic emanation control is not specifically covered, although many of the concepts addressed will be applicable to that area.”

...

The Physical Borderline

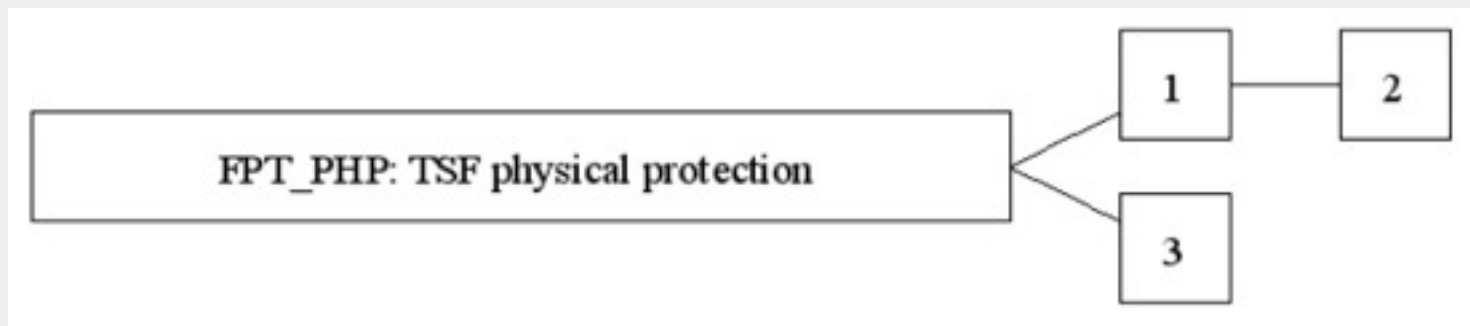
FPT_PHP **physical protection**

“TSF physical protection components refer to restrictions on unauthorised physical access to the TSF, and to the deterrence of, and resistance to, unauthorised physical modification, or substitution of the TSF.

The requirements of components in this family ensure that the TSF is protected from **physical tampering** and interference. Satisfying the requirements of these components results in the TSF being packaged and used in such a manner that physical tampering is **detectable, or resistance** to physical tampering is enforced.

Without these components, the protection functions of a TSF lose their effectiveness in environments where physical damage cannot be prevented. This family also provides requirements regarding how the TSF shall respond to physical tampering attempts”.

The Physical Borderline



FPT_PHP.1 Passive detection of physical attack, provides for features that indicate when a TSF device or TSF element is subject to tampering. However, notification of tampering is not automatic; an authorised user must invoke a security administrative function or perform manual inspection to determine if tampering has occurred.

FPT_PHP.2 Notification of physical attack, provides for automatic notification of tampering for an identified subset of physical penetrations.

FPT_PHP.3 Resistance to physical attack, provides for features that prevent or resist physical tampering with TSF devices and TSF elements.

The Physical Borderline

CCRA CPL and Physical Attacks

Hardware Products & PPs certified by CCRA schemes with resistance to physical attacks as a key security objective:

- Smartcards,
- IDS appliances,
- HSMs,
- IP crypto devices,
- TPMs,
- Photocopiers,
- Handheld devices,
- etc.

Main observation: physical protection is outside the TOE objectives and SFRs, the evaluation scope is limited to the “logical” or software part of the TOE.

→ In general only included in **smartcard ICs** able to resist high attack potential pentesting.

“Security Boxes”

A proposal for “Security Box” definition

“**security**” = “TOE self-protection against attackers with direct access”

“**box**” = “high scale physical envelopment with counter-measures”

→ outside microelectronic components, e.g. not a smartcard IC

Sec-Box → hardware TOE + soft/firmware + shieldings

“**shielding**” = combination of chemical, metallic, etc (passive and active) elements

Examples of TOEs with sec-box:



- the hardware box of a router
- IP crypto devices,
- ruggedized CPUs,
- etc.etc.



Sec-Box Counter-measures

Typical Sec-Box Counter-measures

The “security box” of the TOE is composed of physical protection counter-measures based on **hardware and software active mechanisms**. Usually these mechanisms involve **also passive protections** as an inherent part of the security functionality they provide. Examples of this mechanisms are:

- metallic shields or armours,
- wire meshes,
- chemical protections like epoxy resin,
- etc. etc.

in conjunction with **sensors and electronic anti-tamper mechanisms** to provide operations like:

- secure data erasing,
- alarm generation,
- component destruction,
- etc.etc.

Sec-Box Counter-measures

Opening sensors: contact switches and flaps

The opening sensors used to have the form of **contact switches** or **micro flaps** located in strategic locations and key points of the physical box. While the box is closed they maintain a sensor physically pressed, but when the box is opened or broken during a physical attack the sensor is released and the sensor detects the aperture transmitting an electronic signal to the TOE in order to perform active actions to notify the security alert or to do any protective actions.

Example:



Closed equipment

Internal sensor

Piece fixed to the box

Open equipment

Internal sensor

Piece fixed to the box



Sec-Box Counter-measures

Passive and Active Shields

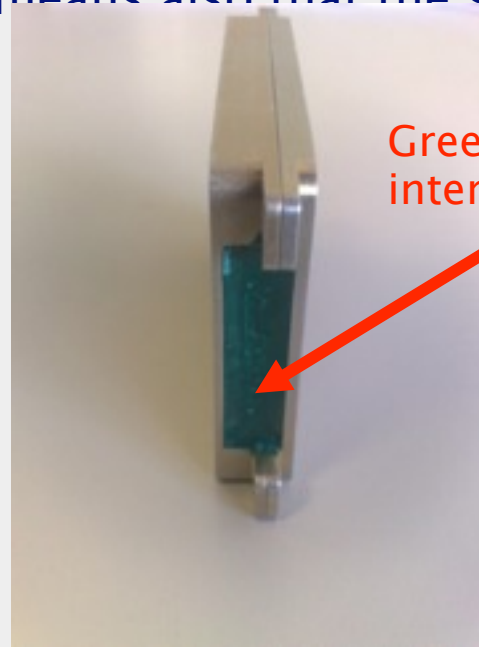
Passive shields can be strong rigid armors made of steel or iron, and/or chemical protections like epoxy resin. Removing them produce the TOE destruction.

Active shields used to be a kind of wire mesh covering the hole surface or specific important elements of the TOE internal architecture. They used to be disposed after the main metallic shield. This mesh can conduct a flow of electrical power connected to sensors in such a way that any attempt to do a cut or hole on it to access the TOE internals means also that the sensors will detect it and start a

Steel armor
protecting a
Multi-chip TOE



Green resin filling the
internals of the TOE



Sec-Box Counter-measures

Other typical sensors

Several additional type of sensors can be placed inside the sec-box.

For instance:

→ **Light** detectors (can be attacked working with the TOE in the dark).

→ **Radiation** sensors e.g. X-ray detectors (problematic to move TOEs through airport detectors,etc.).

→ **Temperature** and climate condition sensors (e.g. can be bypassed using simultaneously different hot/cold sources as for instance the hot from a drilling machine balanced by a liquid nitrogen stream focused on the same point).

All these sensors have as final target to detect manipulations in order to execute emergency actions like the deletion of registers, secrets, crypto keys, destroy the elements, etc.

Non-Destructive Attack Methods

Non-Destructive Testing or Evaluation (NDT/NDE) Methods

Different techniques can be used in order to **identify** the TOE counter-measures when the evaluator has to work assuming operational environments or attack paths where the attacker cannot access to internal information of the TOE.

In such a case the attacker/evaluator can use NDT methods to attack the TOE in a **two-phases strategy** :

- Firstly to identify the counter-measures present in the box,
- Secondly to penetrate the TOE security box bypassing them.

Several techniques have been developed in the status-of-the-art for NDT, and most of them are based on applying physical phenomena like electromagnetic waves, ultrasound waves, subatomic particle emanations, etc. to analyze the TOE internals without doing real damage to it.

Non-Destructive Attack Methods

Visual/Optical Inspections

The **Visual Testing (VT)** is the most simple and old approach to identify counter-measures in the box. It should not be underestimated, and be done firstly.

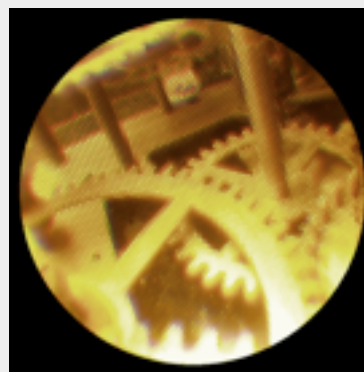
It can start with a **direct** VT when feasible, maybe supported with small “dentist” mirrors or tools to get an appropriate point of view. After the first approximation the process can follow with a **remote** VT using specific optical tools with enough accuracy.

Examples: mirrors, boroscopes, fiberscopes (flexible to access difficult places inside the box) high-resolution cameras, micro-cameras, etc.

Boroscope



Fiberscope



Source: Wikipedia

Non-Destructive Attack Methods

X-Ray Analysis

Use of X-Ray beamers in order to get information about the internal TOE architecture based on its radiographies.

Combining sets of 2D radiographies to get information on the 3D TOE architecture.

Radiographies drawn over films or screens. Specific PC+software can record images and provide image processing tools.

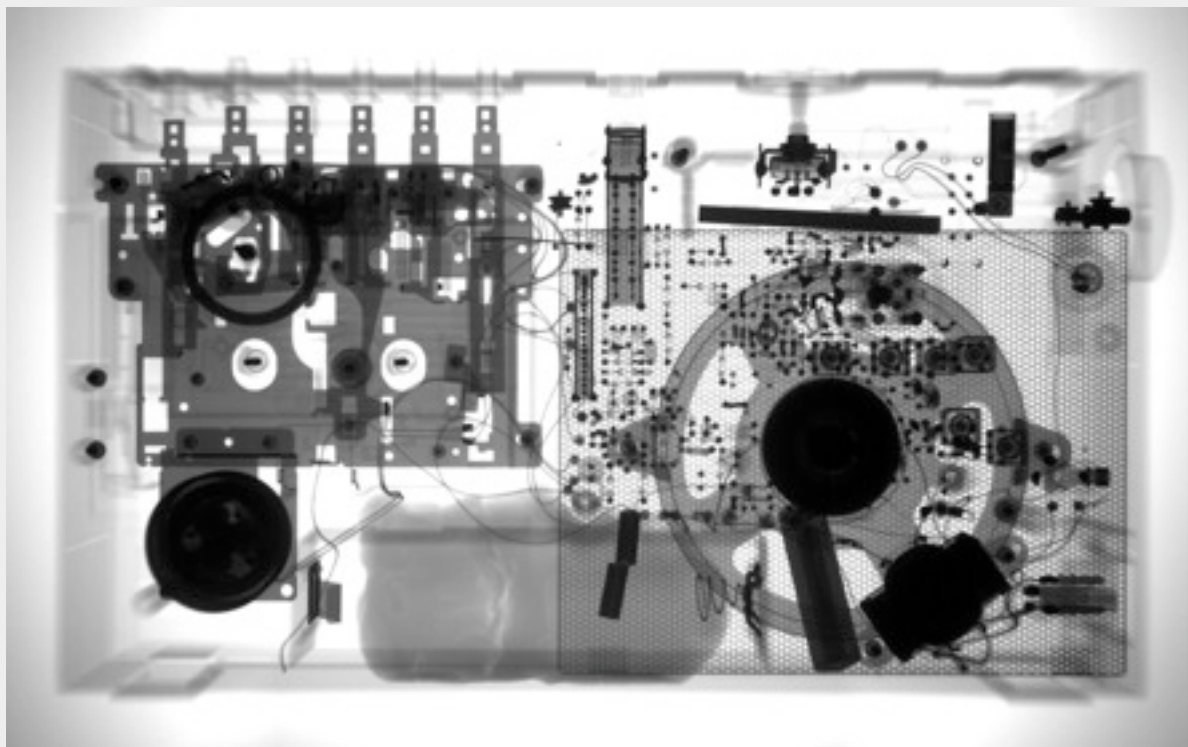
Portable devices do not require a big amount of protectios for the users, maybe just personal radiation detectors.

Better equipments are located in chambers to put equipment inside and perform 3D analysis.

Non-Destructive Attack Methods

X-Ray Analysis

Example: electronic equipment radiography.



Source: VIDISCO

Non-Destructive Attack Methods

X-Ray Analysis

Example: X-Ray portable equipment.



Source: VIDISCO

Non-Destructive Attack Methods

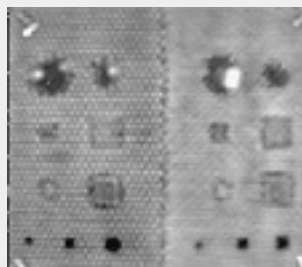
Thermography

Remote acquisition of infrared radiation using thermographic cameras.

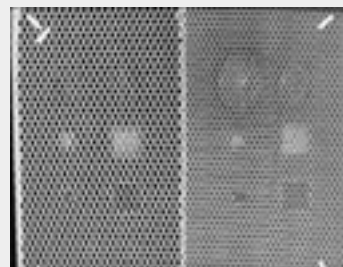
Additional light or hot sources can be used to increase image resolution.

Rarely useful due metallic boxes distribute the temperature in the surface.

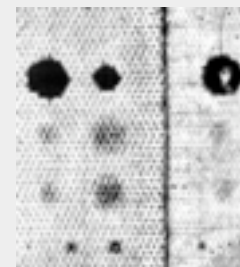
E.g. useful to see through epoxy resins.



Thermography



X-Ray



Ultrasound

Source: Thermalwave.com

Non-Destructive Attack Methods

Ultrasound

Sound waves with frequency beyond the range that can be heard by human beings. (around 20,000 Hz)

Useful to see wires, hardware components, etc. chemical protections. Also to detect breaches and gap in surfaces.

Other techniques

- Laser-Shearography:
- Alternating Current Field Measurement or ACFM.
- Electromagnetic Testing (ET): radar, resonance, micro-waves, etc.
- Penetration using liquids.
- Etc.etc.

Destructive Attack Methods

Penetrating the Physical Shield

Destructive penetration of the steel armour and wire mesh in a TOE can directly be a security problem, without the necessity of any other internal TOE manipulation. For example in certain circumstances it could be used to put a wireless device inside the box in order to generate an information leakage in a TOE where confidentiality was a security object.

Exploiting this kind of vulnerability in a sec-box can be done with different tools:

→ **Simple** sec-boxes can just require the use of standard sets of mechanical hand tools (hammer, screwdriver, etc.).

→ **Standar** sec-boxes can be penetrated using drilling machines with different cutters e.g. diamond-glass cutter, etc. and different RPM 200-3000.

→ **Complex** sec-boxes require the use of several types of milling

Destructive Attack Methods

Penetrating the Physical Shield



Simple milling machine



Milling machine with CNC



Milling cutters



Several drilling cutters for different metals

Source: Wikipedia



Destructive Attack Methods

Penetrating the Chemical Shield

Chemical shield is basically composed of different kinds of resins like **epoxy resin**. These resins are usually put inside the TOE in order to cover the architectural hardware components. The resin hides the components and trying to remove the resin cause the components destruction.

Using thermography or ultrasound it is possible to identify elements inside the resin previously to penetrate it with accuracy.

Usually removing resins involve several techniques like:

- **Mechanic methods:** automatic grinding machines and hand tools.
- **Chemical methods:** techniques very used on smartcard area for IC de-processing. Different acids and chemicals are combined and applied over the resin to do a liquid etching of it.
- **Plasma methods:** dry etching techniques based on plasma beamers like RIE (Reverse Ionized Etching) and so. Also common in the

Method for Vulnerability Analysis

Modelling the Attack Scenarios

TOE located in:

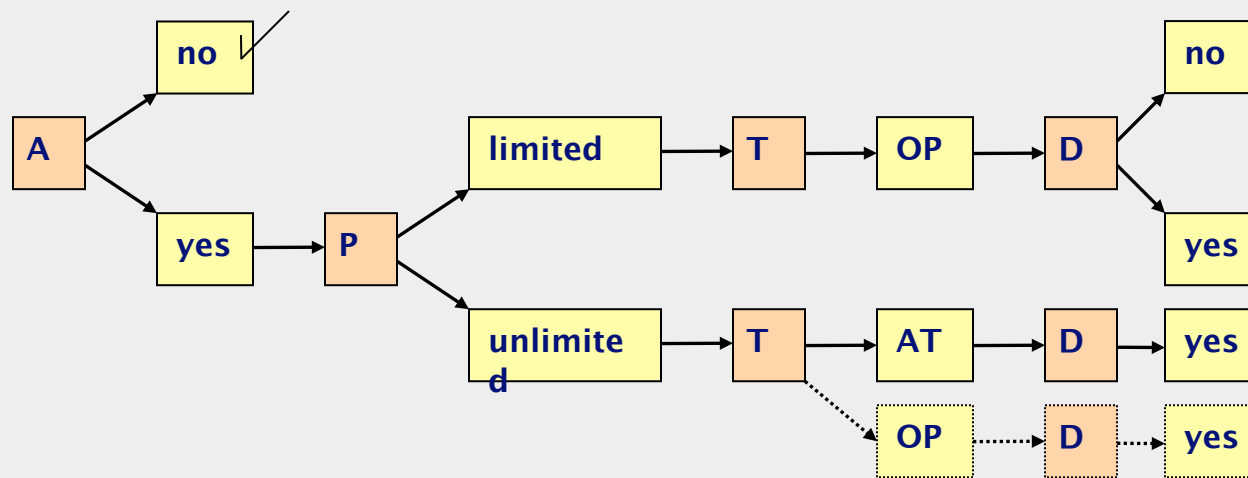
- 1) **“Secure” facilities:** e.g. MoD sites, under continuous monitoring of security guards, with restricted access.
- 2) **Public facilities:** e.g. some Public Administration sites, or computing centres of companies, etc. where some kind of control access exists but there are possibilities of having a potential attacker accessing to the TOE for a limited amount of time (the attacker could manipulate the TOE but not capture or steal it).
- 3) **Mobile platforms:** e.g. TOE operating in a boat, car, bus, BMR, airplane, etc. The access can be restricted but there is always the possibility of having a crash or accident with the platform. During it potential attackers could have access to a part of the TOE or to all of it, and they could steal it to attack without limitations in their own environment.
- 4) **Transport vehicles:** e.g. TOE been transported by the manufacturer in their own vehicles for delivery, etc. There is also the possibility of accidents but in this case the TOE is not operational, it is kept in some “secure” state or not activated yet.
- 5) **Manufacturer facilities:** e.g. during the development phase, or configuration phases. Only authorized personnel can access the TOE.

Method for Vulnerability Analysis

Attack Vector and Attack Paths

Analysing the scenarios, we can define an **attack vector** $V=(A,P,T,D)$ composed of:

- Access to the TOE (A): yes/no accessible to manipulate it.
- Period of time available to manipulate the TOE (P): unlimited/limited (minutes, hours).
- Tools or Equipment to attack (T): OP/AT i.e. limited by the operational environment (OP), or unlimited because they are going to be used in the attacker's own environment or facilities (AT).
- Destructive (D): yes/no the attacker can leave the TOE broken or if he has to leave it operational after tampering (undetected and operational).



Method for Vulnerability Analysis

Attack Paths & Attack Scenarios

Considering each branch in previous tree diagram, we can get to a specific attack scenario to define a set of penetration tests or to put an assumption in the ST:

- A = no → assumption: op.environment restricts the physical attacker access.
 - A = yes → P = limited → T = OP → D = no → define pentests.
 - A = yes → P = limited → T = OP → D = yes → define pentests.
 - A = yes → P = limited → T = AT → ST assumption: op.env. restricts access with T = AT.
 - A = yes → P = unlimited → T = OP → D = no → assumption: op.env. restricts TOE replacement.
 - A = yes → P = unlimited → T = AT → D = no → assumption: op.env. restricts TOE replacement.
 - A = yes → P = unlimited → T = OP → D = yes → define pentests.
 - A = yes → P = unlimited → T = AT → D = yes → define pentests.
- Analysing previous paths we see there are only **3 basic vectors/scenarios**:

- V1** = (A = yes, P = limited, T = OP, D = no) : attacks in TOE's op.environment with limited tools and time to tamper it a leave it again with changes undetected.
- V2** = (A = yes, P = limited, T = OP, D = yes) : attacks in TOE's op.environment with limited tools and time to tamper it a leave it broken e.g. to steal a key or secret stored inside the TOE.
- V3** = (A = yes, P = unlimited, T = AT[OP], D = yes) : capture a TOE operational or not, to attack it in the attacker's facilities using his own equipment with unlimited time or tools and even originating the destruction of it.

Conclusions

→ Sec-boxes used to be part of multi-chip TOEs that should have a security objective for physical attack protection: detect always tampering and probing and go then to a secure state.

→ Parallelism with Attack Methods of Smartcards and similar devices but in a higher scale.

→ There is a necessity of additional guidance for the application of CEM in evaluations of hardware TOEs including Sec-boxes.

Thank you by your attention
Questions?

* **Contact:**

<http://www.oc.ccn.cni.es>

organismo.certificacion@cni.es



Thank you by your attention
Questions?

* **Contact:**

<http://www.oc.ccn.cni.es>

organismo.certificacion@cni.es

