Álvaro Ortega Chamorro
Epoche & Espri
eval@epoche.es

EPOCHE & ESPRI

Hardware Security

Attack Methods for HW devices with Security Boxes

Common Criteria

Agenda

EPOCHE & ESPRI

- Introduction
- Technology overview
- Main Tamper Concepts
- CEM Methodology
- General HW Attack Methods
- Product-based methodology
- Bloopers
- Conclusions

Introduction (i)

EPOCHE & ESPRI

- ✓ CC excludes evaluation of some hardware aspects

  → Rephrase the CC to embrace HW evaluations

- ✓ 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, POIs.

Introduction (ii)

EPOCHE & ESPRI

- ✓ Different characteristics but common techniques

  → Include in the CEM a general framework:

  - ➢ Evaluation of HW features
  - ➢ Compatible with the existing VA and attack potential ratings

Introduction (iii)

EPOCHE & ESPRI

Proposal

- ✓ CEM General framework *"TSF physical protection (FPT_PHP)"*
  - ❖ Evaluation of HW features
  - ❖ Compatible with existing VA and attack potential ratings

Up to AVA_VAN.4

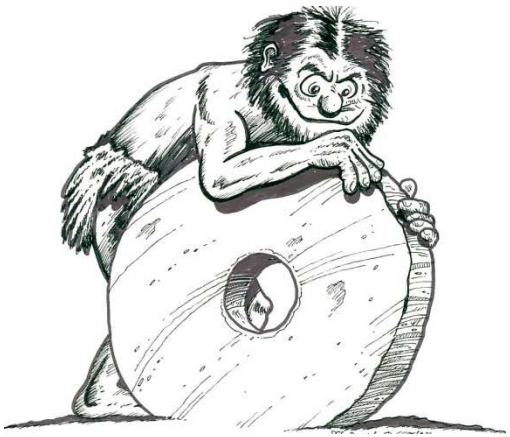
- ✓ Supporting document
  - ✓ General Attack Methods
  - ✓ Particular Attack Paths

AVA_VAN.5

Technology Overview (i)

EPOCHE & ESPRI

- ✓ The wheel is already invented
- ✓ Combination of mechanisms
- ✓ From Smartcards to Security Boxes

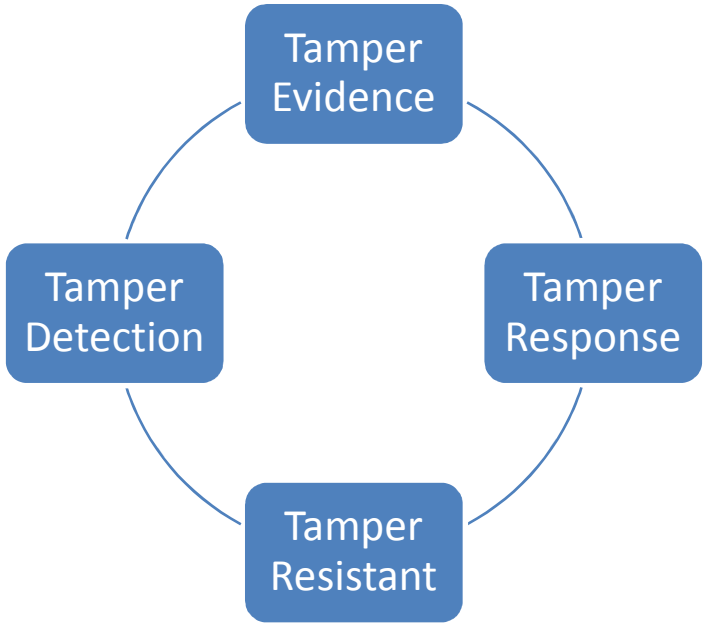


Technology Overview (ii)

EPOCHE & ESPRI

- ✓ Common characteristics
- ✓ Common assets
- ✓ Common assumptions

Main Tamper Concepts



Mechanisms to achieve these properties?

CEM Methodology (i)

EPOCHE & ESPRI

Proposal Methodology for FPT_PHP

FPT_PHP.2 Notification of Physical Attack

→ Verify that the tamper evidence mechanisms are effective by trying to modify the TOE without leaving evidence.

→ Test each tamper detection mechanism, in order to verify that the notifications take place as expected.

FPT_PHP.3 Resistance to Physical Attack

→ Simulate each tampering scenario applied to the contemplated elements, and exercise the TSF in order to verify that its behavior remains with no change.

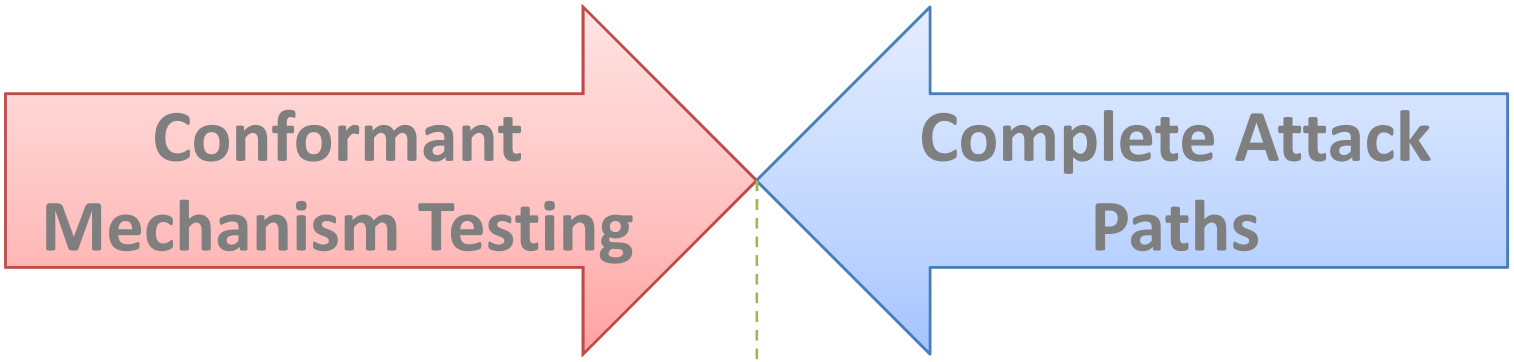
CEM Methodology (ii)

EPOCHE & ESPRI

Parameters to be considered:

Parameter	Enhanced Basic	Moderate
Number of samples	<= 3	<= 6
Elapsed time	<= two weeks	<= one month
Expertise	Not familiarized with HW attacks	Familiarized with HW attacks
Window of Opportunity	Easy access to the device	Easy access to the device
Equipment	Small pliers, hummer, screw driver, chisels, file.	Comercial Drilling machine, comercial chemical dissolvents

General HW Attack Methods (i)



- ✓ Isolated Mechanisms
- ✓ Concurrent testing
- ✓ Design factors?

- ✓ More realistic
- ✓ Know-How dependent
- ✓ Design tested

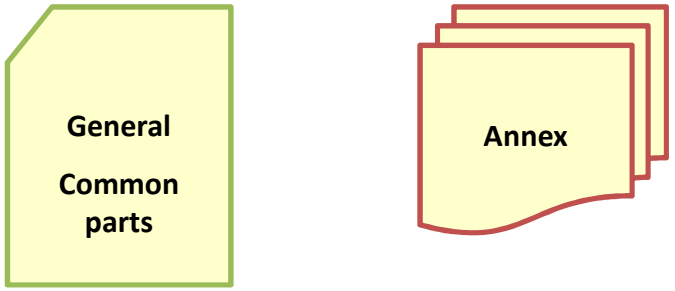
General HW Attack Methods (ii)

EPOCHE & ESPRI

Attack Categorization

- ✓ Non-Invasive attacks
- ✓ Invasive attacks

Proposal Structure for the Supporting Document

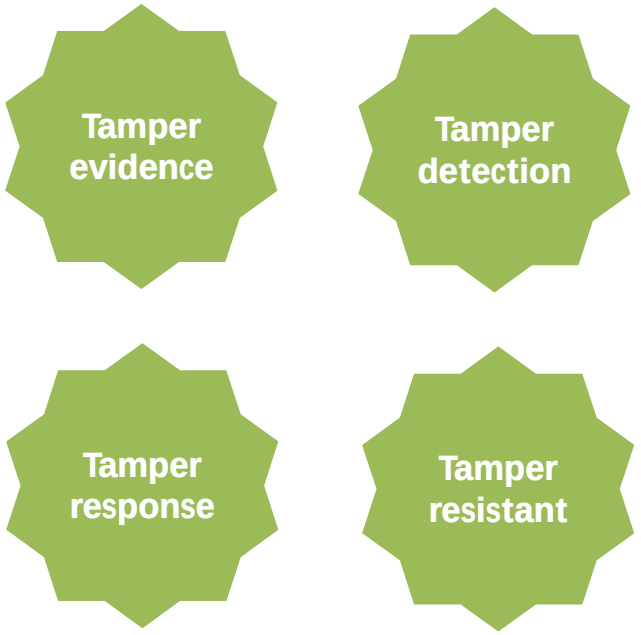


General HW Attack Methods (iii)

EPOCHE & ESPRI

Generic HW Device with countermeasures

- ✓ Hard Steel Case
- ✓ Seals on doors and covers
- ✓ Opening switches
- ✓ Active Mesh
- ✓ Temperature sensors
- ✓ Vibration sensors
- ✓ Potting Material
- ✓ Zeroization Circuitry

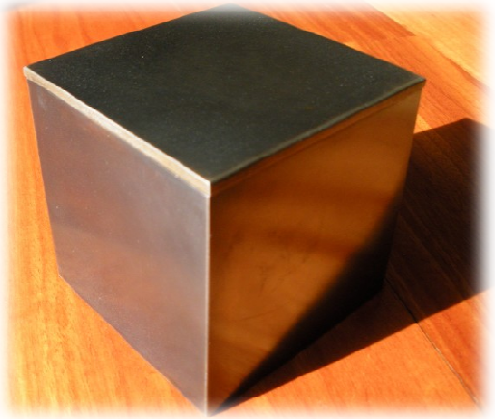


General HW Attack Methods (iv)

EPOCHE & ESPRI

- Hard Steel Case

Milling, drilling or cutting the steel case with the help of proper tools and machines.



Caution factors:

- ✓ High temperature
- ✓ Vibrations
- ✓ Damages to internals
- ✓ Opening switches activation

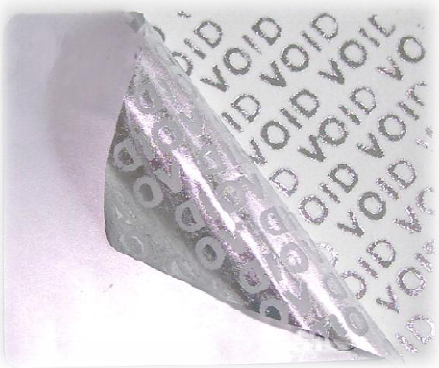
Tamper resistant

General HW Attack Methods (v)

EPOCHE & ESPRI

- Seals on doors

Using a dissolvent under the seal or application of heat to remove it without leaving evidence.



Caution factors:

- ✓ High temperature
- ✓ Damages caused by the dissolvent on the surface where the seal is present
- ✓ Damages on the seal itself

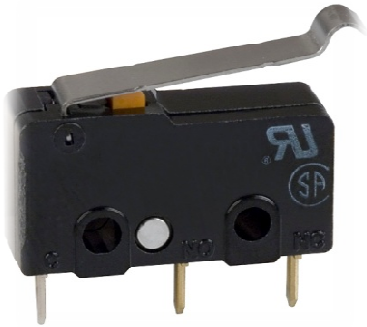
Tamper evidence

General HW Attack Methods (vi)

EPOCHE & ESPRI

❑ Opening Switches

Fix the switch using some kind of glue to avoid the switch activation.



Caution factors:

- ✓ Handle the device carefully in order to avoid the switch activation
- ✓ The glue could damage other components of the device

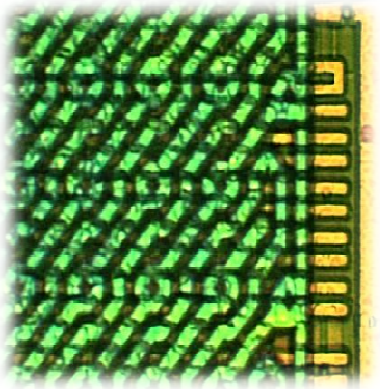
Tamper detection

General HW Attack Methods (vii)

EPOCHE & ESPRI

❑ Active Mesh

Identify the mesh end-points, short-circuit it and provide it with similar electric condition to avoid the detection.



Caution factors:

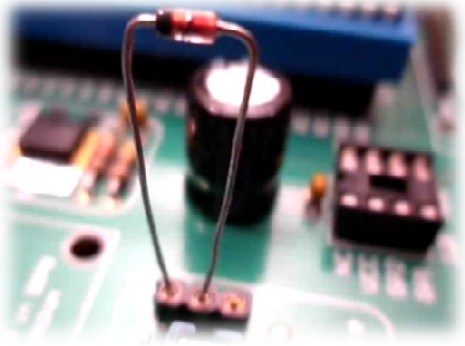
- ✓ Electric behavior of the mesh is required before attack
- ✓ Handle the mesh carefully to avoid cutting or damaging it before deactivation

General HW Attack Methods (viii)

EPOCHE & ESPRI

- Temperature sensor

Attack and handle the device in the range the temperature sensor is not activated.



Caution factors:

- ✓ Other attacks such as drilling could elevate the temperature out of range
- ✓ Avoid disconnecting the sensor to the PCB board.

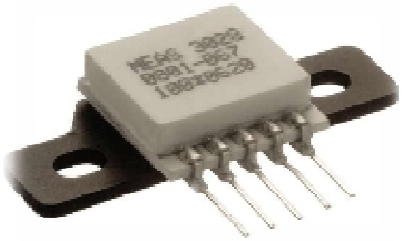
Tamper detection

General HW Attack Methods (ix)

EPOCHE & ESPRI

❑ Vibration sensor

Attack and handle the device avoiding abrupt movements.



Caution factors:

- ✓ Other attacks such as drilling could activate the sensor
- ✓ Avoid disconnecting the sensor to the PCB board.

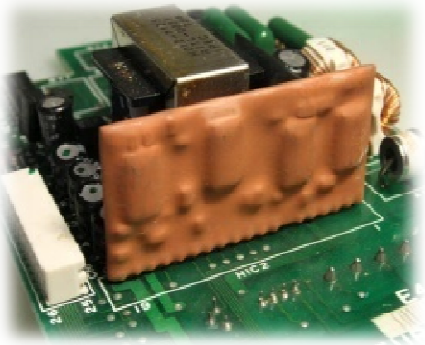
Tamper detection

General HW Attack Methods (x)

EPOCHE & ESPRI

❑ Potting material

Use chemical products to dissolve the potting material. File the material to have access to the ICs.



Caution factors:

- ✓ Chemical product could damage ICs
- ✓ Handling the potting material without care could extract the ICs from the PCB board.

Tamper resistant

General HW Attack Methods (xi)

EPOCHE & ESPRI

❑ Zeroization Circuitry

Destroy zeroization circuitry (e.g. using shaped charge technology) and thus making it not able to be activated. Other option is trying to deactivate it.

Caution factors:

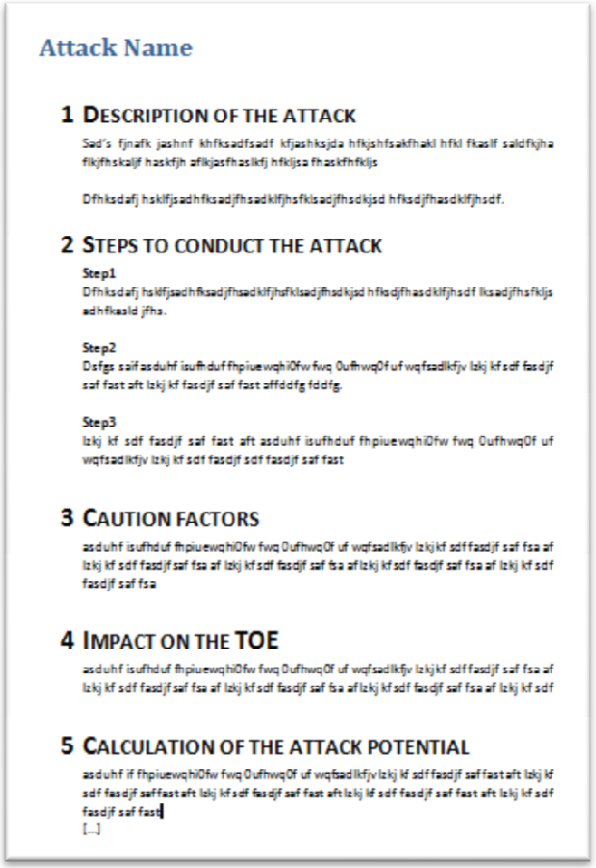
✓ If shaped charge is to be used, avoid destroying other components.

Tamper response

General HW Attack Methods (xii)

EPOCHE & ESPRI

General Supporting Document Structure



Attack Name

1 DESCRIPTION OF THE ATTACK

Sad's fjnafk jashnf khfksadfsadf kfjashksjda hfkjshfsakfhakl hfkl fkaslf saldfkjha flkjfhskaljf haskfjh aflkjasfhaslkfj hfkljsa fhaskfhfkljs

Dfhksdafj hsklfjsadhfksadjfhsadklfjhsfklsadjfhsdkjsd hfksdjfhasdklfjhsdf.

2 STEPS TO CONDUCT THE ATTACK

Step1

Dfhksdafj hsklfjsadhfksadjfhsadklfjhafklsadjfhsdkjsd hfkadjfhasdklfjhsdf lksadjfhsfkljs adhfkasld jfha.

Step2

Dsfgs saif asduhf isufhduf fhpiuewqhi0fw fwq 0ufhwq0f uf wqfsadlkfjv lzkj kf sdf fasdjf saf fast aft lzkj kf fasdjf saf fast affdcfg fdcfg.

Step3

lzkj kf sdf fasdjf saf fast aft asduhf isufhduf fhpiuewqhi0fw fwq 0ufhwq0f uf wqfsadlkfjv lzkj kf sdf fasdjf sdf fasdjf saf fast

3 CAUTION FACTORS

asduhf isufhduf fhpiuewqhi0fw fwq 0ufhwq0f uf wqfsadlkfjv lzkjkf sdf fasdjf saf fsa af lzkj kf sdf fasdjf saf fsa af lzkj kf sdf fasdjf saf fsa af lzkj kf sdf fasdjf saf fsa af lzkj kf sdf fasdjf saf fsa af lzkj kf sdf fasdjf saf fsa

4 IMPACT ON THE TOE

asduhf isufhduf fhpiuewqhi0fw fwq 0ufhwq0f uf wqfsadlkfjv lzkjkf sdf fasdjf saf fsa af lzkj kf sdf fasdjf saf fsa af lzkj kf sdf fasdjf saf fsa af lzkj kf sdf fasdjf saf fsa af lzkj kf sdf

5 CALCULATION OF THE ATTACK POTENTIAL

asduhf if fhpiuewqhi0fw fwq 0ufhwq0f uf wqfsadlkfjv lzkj kf sdf fasdjf saf fast aft lzkj kf sdf fasdjf saf fast aft lzkj kf sdf fasdjf saf fast aft lzkj kf sdf fasdjf saf fast aft lzkj kf sdf fasdjf saf fast

[...]

Product-based Methodology (i)

EPOCHE & ESPRI

Smart Meters

- ✓ Countermeasures to provide Tamper-Detection capabilities.
- ✓ If tamper is detected, the energy company will be advised.
- ✓ The threats comes from the customer itself.

Product-based Methodology (ii)

EPOCHE & ESPRI

Digital Tachograph

- ✓ Countermeasures to provide Tamper-Detection and Tamper-Resistant capabilities.
- ✓ The system must remain in active mode to not raise suspicion.
- ✓ The threats comes from the driver itself.

Product-based Methodology (iii)

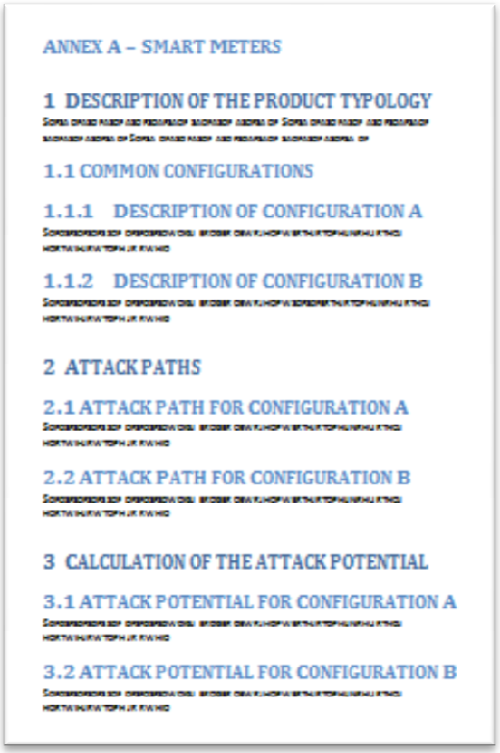
EPOCHE & ESPRI

PIN Entry Devices

- ✓ Countermeasures to provide tamper detection capabilities.
- ✓ The asset is the PIN inserted by the customer.
- ✓ Multiple threats must be covered for this kind of devices.

Product-based Methodology (iv)

Annex structure



ANNEX A – SMART METERS

1 DESCRIPTION OF THE PRODUCT TYPOLOGY

1.1 COMMON CONFIGURATIONS

1.1.1 DESCRIPTION OF CONFIGURATION A

1.1.2 DESCRIPTION OF CONFIGURATION B

2 ATTACK PATHS

2.1 ATTACK PATH FOR CONFIGURATION A

2.2 ATTACK PATH FOR CONFIGURATION B

3 CALCULATION OF THE ATTACK POTENTIAL

3.1 ATTACK POTENTIAL FOR CONFIGURATION A

3.2 ATTACK POTENTIAL FOR CONFIGURATION B

Bloopers

EPOCHE & ESPRI

- ✓ Active mesh not covering the total perimeter of the device.
- ✓ Use of Plasticine to surround ICs, and then apply Potting Material.
- ✓ Huge ranges for temperature sensors.
- ✓ Opening switches placed in absurd locations.
- ✓ Use of easily replaceable seals

Conclusions

EPOCHE & ESPRI

- Increasing relevance of HW protection mechanisms in devices with SECBOX → Rephrase CC to include HW evaluations.

- Common methodology needed
  - In CEM, up to AVA_VAN.4
  - Supporting document for AVA_VAN.5

- Expertise-dependent tools and techniques used

Álvaro Ortega Chamorro
eval@epoche.es

Epoche & Espri, S.L.U.
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