



EPOCHE & ESPRI

Physical protection: Anti-tamper mechanisms in CC security evaluations

10ICCC Norway

Agenda



E P O C H E & E S P R I

- Physical protection requirements in CC documentation.
- Architecture Design in CC documentation.
- Main tamper concepts.
- Anti-tamper mechanisms.
- Attack methods for anti-tamper mechanisms.
- Comparison with FIPS 140-2.
- Conclusions.



1. Introduction

- Is CC complete enough at the HW side?
- Which are the critical points we have to focus on to perform a well HW based evaluation?
- Is “tampering” covered by CC as well as needed in nowadays IT market?



2. Physical protection requirements in CC documentation

- **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 authorized user must invoke a security administrative function or perform manual inspection to determining 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."*

3. Architecture Design in CC documentation

Self Protection

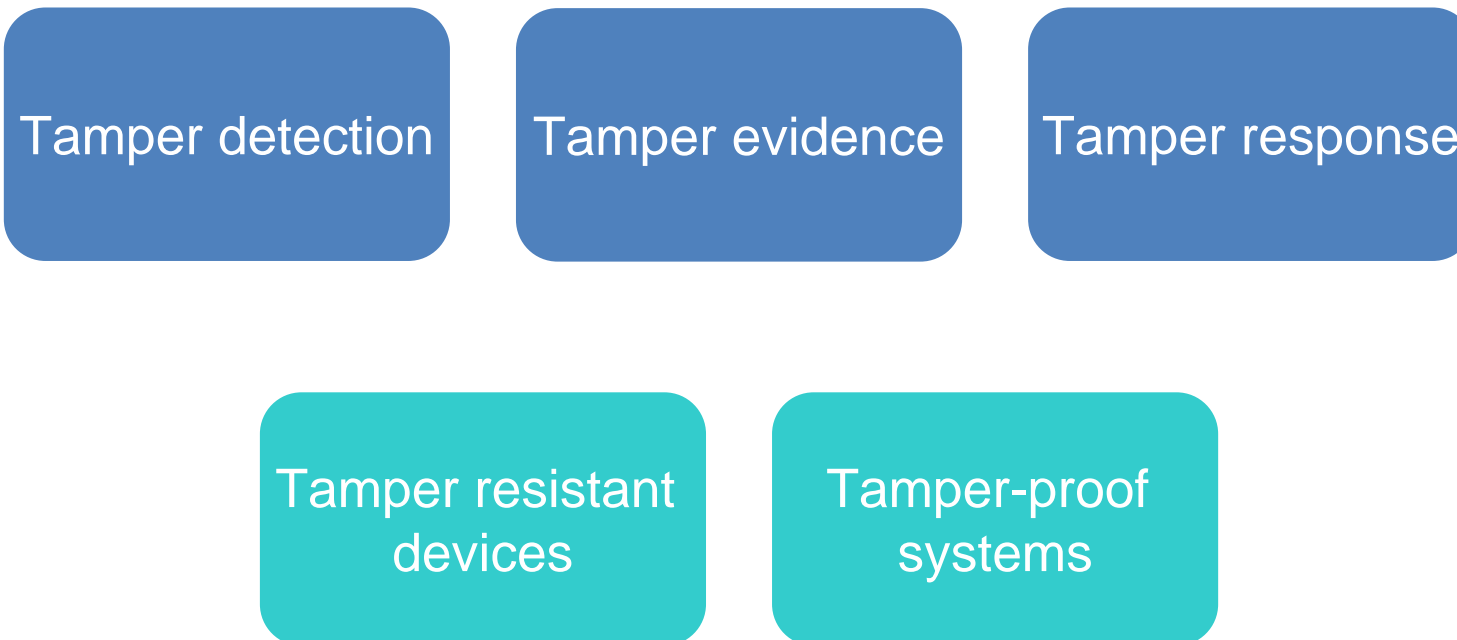
Ability to protect itself from manipulation from external entities that may result in changes to the TSF.

Non-bypassability

This is a property that the security functionality of the TSF (as specified by the SFRs) is always invoked and cannot be circumvented when appropriate for that specific mechanism.



4. Main tamper concepts



5. Anti-tamper mechanisms

MECHANISM	Tamper indicating devices: Seals and Labels
CATEGORY	TAMPER EVIDENCE

- Used to provide evidence of an unauthorized opening of the device.
- Are comprised of a paper and an adhesive.
- Are not designed to resist, instead, they record that an opening attempt took place.
- Must have a unique (tag-like) characteristic or “fingerprint”, such as a serial number.
- Paper damage indicates the opening attempt.



5. Anti-tamper mechanisms

MECHANISM	Uniquely shaped screw heads
CATEGORY	TAMPER RESISTANT DEVICES

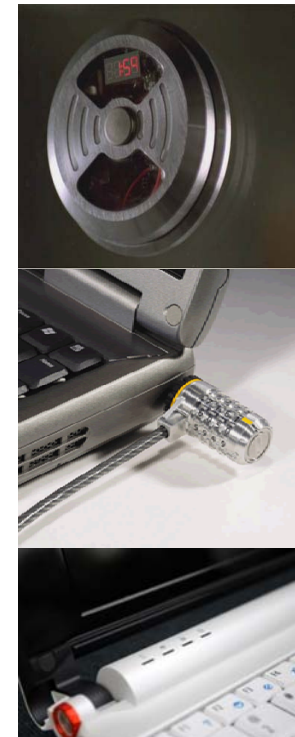
- Uniquely shaped screw heads provide an additional physical barrier, due to the hardness of unscrewing them.
- Opening an enclosure which contains uniquely shaped screw heads with a usual screw driver should be impossible, and this feature provides a tamper resistant mechanism to the protected device.



5. Anti-tamper mechanisms

MECHANISM	Locks for removable covers and doors
CATEGORY	TAMPER RESISTANT DEVICES

- Provide some prevention of an attack.
- Removing a lock without having the key to the lock, or knowing the lock's logical combination, requires a considerable amount of force.
- The advantage of tamper evident seals over pick-resistant locks is that they will provide indication of unauthorized access unless a sophisticated attack method is successful.



5. Anti-tamper mechanisms

MECHANISM	Coating: encapsulation materials
CATEGORY	TAMPER RESISTANT DEVICES & TAMPER DETECTION

- The device may be covered with a coating such that attempting to peel or pry the coating from the device will have a high probability of resulting in serious damage to the device.
- The tamper-evident coating or tamper-evident enclosure can be opaque within the visible spectrum.
- The four main mechanisms employed are:
 - Epoxy Resins
 - Conformal Coatings
 - Bleeding Paint
 - Metal or hard plastic enclosure



5. Anti-tamper mechanisms

MECHANISM	Mechanical mechanisms
CATEGORY	TAMPER DETECTION & TAMPER RESPONSE

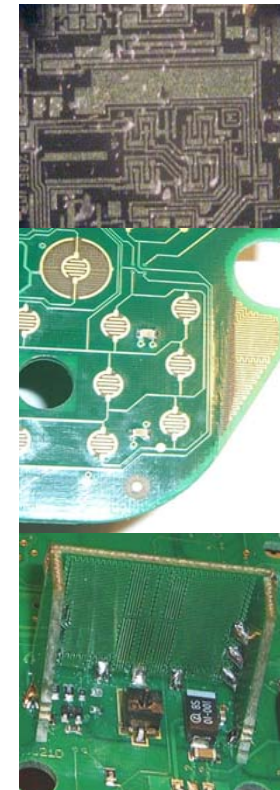
- Provide the capability of opening detection. Each device may employ this feature to perform different actions.
- Switches provide tamper detection, and in some cases, tamper response mechanism.
- There are many different types of switches, but most of them are directly installed under the enclosure of the device wanted to be protected.



5. Anti-tamper mechanisms

MECHANISM	Protective Sensor Mesh Wall
CATEGORY	TAMPER DETECTION

- Usually employed to detect a drilling attack.
- Contain a complex circuitry which is easy to be broken when trying to drill it. Once broken, the device detects this attempt, and performs the consequent action.



5. Anti-tamper mechanisms

MECHANISM	Use of brittle components
CATEGORY	TAMPER DETECTION & TAMPER RESPONSE

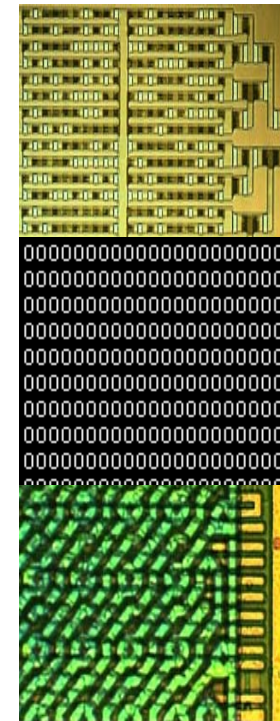
- Brittle components provide high probability of causing serious damage to the device in case of penetration attempts (i.e. the device will not function).
- Usually, these kinds of mechanisms are installed in critical devices which may only work under concrete environment circumstances.



5. Anti-tamper mechanisms

MECHANISM	Zeroization circuitry
CATEGORY	TAMPER RESPONSE

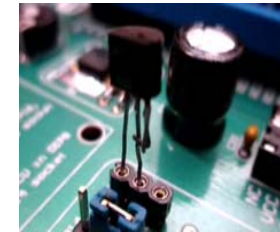
- Common response mechanism. Secret data is deleted.
- Two kinds of zeroization mechanism:
 - Passive zeroization.
 - Active zeroization.
- Tamper response and zeroization circuitry.



5. Anti-tamper mechanisms

MECHANISM	Sensors
CATEGORY	TAMPER DETECTION & TAMPER RESPONSE

- The device may have different types of sensors:
 - Voltage
 - Frequency Temperature
 - Light (or other radiation)





6. Attack methods for anti-tamper mechanisms

MECHANISM	Overcoming Sensors
CATEGORY	NON-INVASIVE

- Deactivating, behavior modification or bypass of the sensors or filters used by the device to monitor the environmental conditions and to protect itself from conditions that would threaten correct operation of the device.



6. Attack methods for anti-tamper mechanisms

MECHANISM	Weaknesses when zeroizing
CATEGORY	NON-INVASIVE

- Passive zeroization may not be sufficient because of data permanence, where previously stored state remains in RAM cells and other storage media after they have lost power. Ionic contamination, hot-carrier effects, and electromigration can 'imprint' the stored state over time and extreme temperature or voltage may cause RAM content to remain for seconds or even minutes after power is removed.



6. Attack methods for anti-tamper mechanisms

MECHANISM	Chemical attacks on tamper evident Seals
CATEGORY	NON-INVASIVE

- Use of a solvent on the adhesive.
- Depends on the type of paper utilized in the seal.
- Acids and bases may not be effective in removing tamper evident seals.



6. Attack methods for anti-tamper mechanisms

MECHANISM	Physical shield penetration
CATEGORY	INVASIVE

- Bypassing the physical shield.
- A physical attack could be drilling the device enclosure or trying to open it.
- Depending on the kind of tamper detection mechanism installed on the device, it will or won't be possible to perform a success attack.



6. Attack methods for anti-tamper mechanisms

MECHANISM	Chemical attacks on Coatings
CATEGORY	INVASIVE

- Attacks on coatings are those common to polymers.
- One polymer attack that potentially could work on a coating is the breaking of the polymer chemical bonds with an ultraviolet light source
- To prevent the decomposition of the coating in sunlight, some coatings have included in them a UV stabilizer.



6. Attack methods for anti-tamper mechanisms

MECHANISM	Attacks on pick resistant locks
CATEGORY	INVASIVE

- Cutting of an external lock's shackle with a hacksaw.
- Drilling out of a lock incorporated into an enclosure.
- The stealing of the lock's key or the discovery of the lock's combination through shoulder surfing, will allow an attacker to open the enclosure's door or remove its cover without detection.



7. Other standards: FIPS 140-2 Physical Security

	General Requirements for all Embodiments	Single-Chip Cryptographic Modules	Multiple-Chip Embedded Cryptographic Modules	Multiple-Chip Standalone Cryptographic Modules
Security Level 1	Production-grade components (with standard passivation).	No additional requirements.	If applicable, production-grade enclosure or removable cover.	Production-grade enclosure.
Security Level 2	Evidence of tampering (e.g., cover, enclosure, or seal).	Opaque tamper-evident coating on chip or enclosure.	Opaque tamper-evident encapsulating material or enclosure with tamper-evident seals or pick-resistant locks for doors or removable covers.	Opaque enclosure with tamper-evident seals or pick-resistant locks for doors or removable covers.
Security Level 3	Automatic zeroization when accessing the maintenance access interface. Tamper response and zeroization circuitry. Protected vents.	Hard opaque tamper-evident coating on chip or strong removal-resistant and penetration resistant enclosure.	Hard opaque potting material encapsulation of multiple chip circuitry embodiment or applicable Multiple-Chip Standalone Security Level 3 requirements.	Hard opaque potting material encapsulation of multiple chip circuitry embodiment or strong enclosure with removal/penetration attempts causing serious damage.
Security Level 4	EFP or EFT for temperature and voltage.	Hard opaque removal-resistant coating on chip.	Tamper detection envelope with tamper response and zeroization circuitry.	Tamper detection/ response envelope with tamper response and zeroization circuitry.

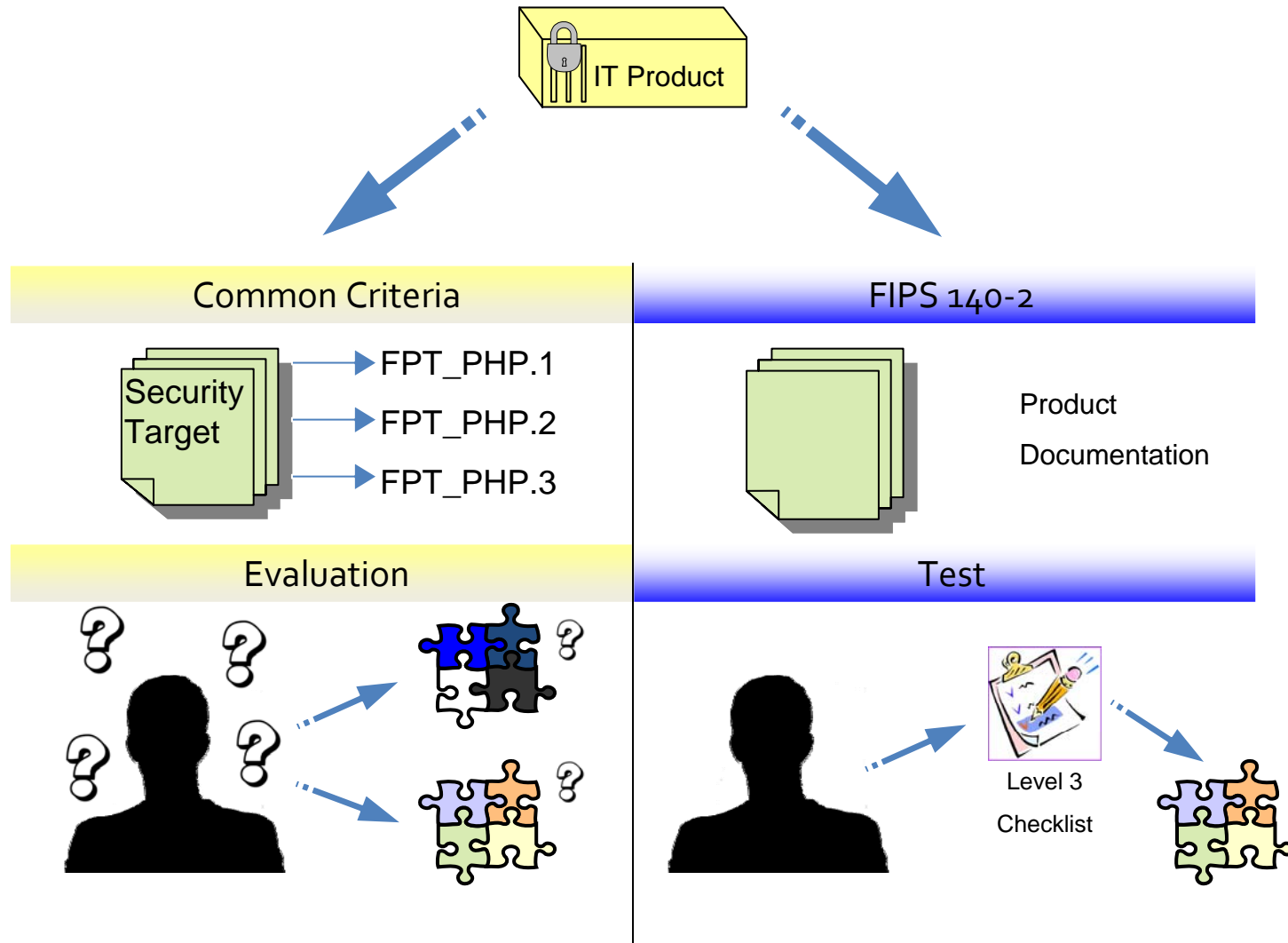


Specific anti-tamper mechanisms

8. Tamper mechanisms: CC vs. FIPS 140-2

	Common Criteria		FIPS 140-2	
	Requirement	Mechanisms	Level	Mechanisms
Tamper Detection	FPT_PHP.2	?	Level 3 Level 4	Automatic zeroization when accessing the maintenance access interface. Tamper response and zeroization circuitry. Protected vents.
Tamper Evidence	FPT_PHP.1	?	Level 2 Level 3 Level 4	Cover, enclosure, or seals.
Tamper Response	FPT_PHP.3	?	Level 3 Level 4	Automatic zeroization when accessing the maintenance access interface. Tamper response and zeroization circuitry. Protected vents.

8. Tamper mechanisms: CC vs. FIPS 140-2





9. Conclusions

- The existence of a supporting document containing a matching between anti-tamper mechanisms and PHP requirements should help.
- Anti-tamper mechanisms employed nowadays are standard enough to be easily covered by CC documentation.
- The ambiguous way of HW evaluation should disappear if CC methodology covers accurately these anti-tamper mechanisms.



EPOCHE & ESPRI

QUESTIONS





EPOCHE & ESPRI

Thanks!

Álvaro Ortega Chamorro
eval@epoche.es