
I-0433: Design Abstractions For Non-IT Mechanisms

TYPE: Guidance
NUMBER: I-0433
STATUS: Ready for External Repost after Interpretations Board Rework/Review

TITLE: Design Abstractions For Non-IT Mechanisms

FIRST POST: [\[cc-cmt 00557\]](#)
MOST RECENT REPOST: [\[cc-cmt 00722\]](#)
COMMENTS DUE BY: Friday, February 6, 2004 to cc-cmt@nist.gov

RELATED TO: <None>

ISSUE:

How are the different levels of design abstractions to be provided for those portions of the TSF that are implemented through non-IT mechanisms, such as physical enclosures or mechanical-tumbler locks? What is the meaning of high-level and low-level design in such contexts?

For example, suppose a TOE claims that FPT_PHP is met by a 2-inch thick steel box protected by an ANSI Level 2 tumbler lock? What levels of design abstraction are required for this? Now suppose the door had been modified to have a magnetic switch that, when the door was open, sent an interrupt to the CPU (similar to a house alarm)? Does that change the answer?

STATEMENT

Assurance methods applied to Information Technology (IT) may require modification when used with non-IT mechanisms. For example, if a non-IT mechanism is claimed as part of the TSF (i.e., it is necessary to satisfy an SFR), then the design information must be provided at an appropriate level of detail to provide the requisite level of confidence that fits with the assurance level in the correct operation of the mechanisms. For simple mechanisms, not all three levels of abstraction (ADV_HLD, ADV_LLD, ADV_IMP) need to be different.

SUPPORT:

The full name of the Common Criteria makes it clear that it is for the evaluation of "Information Technology". The CC doesn't explicitly define the term "Information Technology", although it implies that the term is focused on hardware, software, and firmware mechanisms, where the word "hardware" is used in the computer science sense. It notes that the assessment of non-IT related product security properties are best addressed separately, and indicates that except in specific cases, the evaluation of technical physical aspects of IT security is not covered. From this, it is reasonable to deduce that the focus of evaluation should be on the IT mechanisms.

However, the CC does not preclude physical mechanisms for some SFRs. For those SFRs where it is appropriate, addressing the requirements for design decomposition can be confusing. The notions of "high level" and "low level" do not often apply to enclosures or locks; blueprints are not useful implementation specifics for most evaluators.

Note that it may sometimes be difficult to distinguish IT from non-IT. Although the ends of the spectrum are clear (a steel box with no electronics is clearly non-IT, a CPU is clearly IT), the border cases are difficult (such as mechanical mechanisms that send an interrupt to a CPU). The evaluation team must be able to provide a convincing justification for the IT/non-IT determination in such borderline cases.

The guidance from CCEVS is to use common sense. Take the abstraction to a level appropriate for the mechanism and assurance level. Provide rationale to justify that the level chosen is appropriate.