
I-0433: Design Abstractions For Mechanical Mechanisms

TYPE: Guidance
NUMBER: I-0433
STATUS: Ready for External Review

TITLE: Design Abstractions For Mechanical Mechanisms
COMMENTS DUE BY: Tuesday, July 1, 2003 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 mechanical mechanisms, such as physical enclosures or hardware? What is the meaning of high-level and low-level design in such contexts?

STATEMENT

Assurance methods applied to information technology need to be used with appropriate modifications when applied to non-IT hardware mechanisms. For example, if a physical mechanism is a part of the TSF, then the design information must be provided at an appropriate level of detail to provide an appropriate level of confidence (based on 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. A PP or ST should not depend solely on the use of strictly physical mechanisms (for example, mechanical locks or enclosures) to implement an SFR; if dependence on such mechanisms is necessary, consideration should be giving to moving the SFR to the operational environment. About the only exception is FPT_PHP, where some mechanical mechanisms may be used.

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.

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.