



Sent on behalf of the Director, CCEVS as Valgram #37, and Labgram #18
On Fri 2/14/03 3:18 PM

Subject: Methodology for components above EAL4

CCEVS was recently questioned on what methodology should be used for assurance components above EAL4. In response, the following interim guidance was provided on the ADV_IMP.2, ADV_RCR.2, and AVA_CCA.1 components. This is how these components are to be used until more structured methodology is available.

For evaluations including these components, validators are asked to pay particular attention in these areas, and keep CCEVS apprised if anything even remotely questionable comes up, so that we can clarify the interim guidance if necessary.

As other EAL4+ components are included in evaluations, causing other such interim guidance to be generated, these will be collected together and made available in an effort to maintain consistency.

ADV_IMP.2

ADV_IMP.2 applies to the entire TSF, rather than only the subset of the TSF required by ADV_IMP.1. Therefore, an evaluation including ADV_IMP.2 should use the methodology for ADV_IMP.1, but applied to the entire TSF.

The evaluator confirms the information provided meets the requirements of the additional content and presentation element (ADV_IMP.2.3C: "The implementation representation shall describe the relationships between all portions of the implementation") by checking the code to be sure that interactions among the portions of the code are identified. The "portions of code" in question are those portions that implement the modules that are identified in the low-level design.

The importance of having all of the implementation representation - rather than only the subset -- becomes apparent not in the evaluation work associated with ADV_IMP itself, but in other components. For example, the correspondence between the description of interactions among the modules in the low-level design and the interactions of the portions of the code that implement these modules will be performed as part of ADV_RCR; this ADV_IMP action makes sure the necessary input for that activity is available. Similarly, with the entire implementation representation available, the vulnerability analysis is much more straightforward and lucrative because the evaluator can trace through the code without running into dead ends that would otherwise result from portions of code being unavailable.

ADV_RCR.2

At EAL5, only the Functional Specification and High-Level Design are provided in a semiformal format. ADV_RCR.2 imposes a correspondence determination between these semiformal representations. For all remaining representations that are informal, there must likewise be a correspondence determination. The correspondence determination (at both the semiformal and informal levels) is done in accordance with the methodology for ADV_RCR.1.

AVA_CCA.1

There is no CCA methodology available in the CEM. Until methodology is available, the evaluator confirms the information provided meets the requirements of the content and presentation elements (AVA_CCA.1.1E) using the guidance provided in the Rainbow Document "A Guide to Understanding Covert Channel Analysis of Trusted Systems", November 1993, NCSC_TG-030.

The evaluator confirms that the covert channel analysis shows that the TOE meets its functional requirements (AVA_CCA.1.2E) only for TOEs claiming FDP_IFF.1/FDP_IFC.1 - these are the only functional requirements for which covert channels are meaningful. The policy quoted in these functional components is examined and the evaluator notes any covert channels that violate this policy, including the bandwidth of all such channels. When conducting the covert channel analysis, the evaluator needs to make sure that **all** resources (not just those defined in the applicable FDP_IFC/IFF components) are considered as part of the analysis; if they determine that a resource can be used in a covert channel, yet its use doesn't circumvent the policy set forth by the rules in FDP_IFC/IFF, that covert channel can be ignored.

All channels identified during the covert channel analysis are then included in the testing (AVA_CCA.1.3E).