
I-0382: TSF Architectural Protections Are Really Assurances

NUMBER: I-0382
STATUS: Posted for External Review
TYPE: Request for Interpretation

TITLE: TSF Architectural Protections Are Really Assurances
COMMENTS DUE BY: Monday, February 5, 2001 to IWG@gibraltar.ncsc.mil

SOURCE REFERENCE: CC v2.1 Part 2 Subclause 10.10 FPT_RVM
CC v2.1 Part 2 Subclause 10.11 FPT_SEP
CC v2.1 Part 2 Subclause 10.12 FPT_SSP
CC v2.1 Part 2 Subclause 10.15 FPT_TRC
CC v2.1 Part 2 Subclause 10.6 FPT_ITT
CC v2.1 Part 2 Subclause J.10 FPT_RVM
CC v2.1 Part 2 Subclause J.11 FPT_SEP
CC v2.1 Part 2 Subclause J.12 FPT_SSP
CC v2.1 Part 2 Subclause J.15 FPT_TRC
CC v2.1 Part 2 Subclause J.6 FPT_ITT
CC v2.1 Part 3
CC v2.1 Part 3 Subclause 10.4 ADV_INT

RELATED TO:
[I-0339](#) Assurance Of RVM Is By Testing And Design Analysis

ISSUE:

Many of the families in the FPT class are really architectural assurances; assurance is gained through design analysis combined with testing through the TOE interface (where possible).

STATEMENT OF INTERPRETATION:

The Common Criteria requires restructuring to properly present those families related to architectural assurances.

PROJECTED IMPACT:

This has a major impact on the structure of the Common Criteria.

SUPPORT:

Background

Many of the families in FPT are "caught in the middle": they are neither clearly functional requirements, nor are they clearly assurance requirements. In versions 1.0 and 2.x of the CC, the placement of these families in Part 2 has been problematic, for it is impossible to verify that the requirements of these components are met solely through testing. True verification requires examination of the design and implementation. Additionally, these families, by their nature, have the characteristic of not having a clear functional interface.

On the other hand, the problematic families do not belong in the Part 3 ADV class. The ADV class deals with the decomposition of the design from the high-level functional specification to the implementation. Its goal is to provide confidence that all the functions claimed to be present through the interface are properly implemented. The elements in the Class ADV components are verified solely through design inspection.

The families of particular interest, in CC v2.1 nomenclature, are FPT_RVM and FPT_SEP. These have the characteristic that verification of correctness requires both analysis of design and implementation as well as selective testing.

Investigation for this interpretation also uncovered ADV_INT as a family that is out of place. ADV_INT does not belong in the ADV class, because it is unique in that it places requirements on how the TOE is implemented, not on how the TOE is designed. In this aspect, it is similar to FPT_SEP and FPT_RVM, which also place requirements on implementation.

Potential Solutions

There are four potential solutions to the problems of these components:

1. *Leave things as they are.* This solution has the problem that all the known confusions remain: how are the requirements of the families completely tested through the interface?
2. *Correct the dependencies.* This solution proposed to perform additional dependency analysis to more properly identify the dependencies between functions and assurance. This would allow better identification of the dependencies of EALs upon certain architectural and functional features. However, it fails to show the different approaches to gaining assurance for the indicated components.
3. *Creation of a new Assurance Class.* This solution moves the problematic component into a distinct class for architectural assurances. This distinct class has the common characteristic that assurance is gained through a combination of testing and design analysis.
4. *Creation of a new "Part".* This would create a new part of the Common Criteria for such families that is neither functional nor assurance, but is a hybrid.

Recommendation

The IWG believes that the third approach, creation of a new class, is an acceptable compromise. The first two approaches do not serve to clarify the current confusions, although the notion of showing dependencies of EALs to functions such as RVM and SEP is intriguing. The last approach is too radical. By creating a new class for architectural assurances, it becomes clear that assurance for these families is achieved through a combination of architectural analysis and testing.

Specifically, the IWG proposes restructuring the CC to create in Part 3 a new Architectural Assurances class (NIAP-0382-AAR). This class would contain the current ADV_INT (to be renamed NIAP-0382-AAR_INT) family on Design Internals, as well as the FPT_RVM and FPT_SEP families currently in FPT. Additionally, if FPT_ITT, FPT_SSP, and FPT_TRC have not been incorporated into FPT_SEP (per I-0380), they should be in NIAP-0382-AAR also. The following families should also be reviewed to see if they are more appropriate for NIAP-0382-AAR: FPT_FLS, FPT_AMT, FPT_RCV.

The structure of each new family would be roughly as follows ("xxx" is SEP, RVM, etc.):

OBJECTIVES

This would be a paraphrase of the current objectives of the family, reworked to put the emphasis on design characteristics as opposed to TOE functional behavior.

COMPONENT LEVELING

Similar to the functional leveling

APPLICATION NOTES

Similar to current application notes

NIAP-0382-AAR_xxx.1 TITLE

Dependencies: *As appropriate*

Developer Action Elements:

NIAP-0382-AAR_xxx.1.1D. The developer shall provide the design of the TSF.

Content and Presentation of Evidence Elements:

NIAP-0382-AAR_xxx.1.1C. The design of the TSF shall demonstrate that *functional elements recast as design requirements*

Evaluator Action Elements

NIAP-0382-AAR_xxx.1.1E. The evaluator shall confirm that the information provided meets all requirements for content and presentation of elements.

NIAP-0382-AAR_xxx.1.2E. The evaluator shall test the architectural characteristics called out by this component that are visible through the TSFI.

Inclusion in Assurance Levels

If the goal is to preserve the current CC EAL structuring, none of these NIAP-0382-AAR components should be included in an EAL, except NIAP-0382-AAR_INT (which was previously included in EALs as ADV_INT). This allows their inclusion to remain at the option of the PP/ST author, as is currently the case for the FPT incarnations.

However, given the importance of NIAP-0382-AAR_SEP to the argument of TSF protection, the IWG strongly supports including the lowest hierarchical component of NIAP-0382-AAR_SEP in all EALs. Additional, given the importance of NIAP-0382-AAR_RVM to ensuring that TSP enforcement functions are invoked and succeed, the IWG strongly supports including the lowest hierarchical component of NIAP-0382-AAR_RVM in all EALs.