
I-0381: Relationship Between FPT_PHP And FMT_MOF

TYPE: NIAP Interpretation
NUMBER: I-0381
STATUS: Approved by TTAP/CCEVS Management
TITLE: Relationship Between FPT_PHP And FMT_MOF
EFFECTIVE: 2002-03-04
SOURCE REFERENCE: CC v2.1 Part 2 Subclause 10.7 FPT_PHP.1
CC v2.1 Part 2 Subclause J.7 FPT_PHP.1
RELATED TO: <None>

ISSUE:

Management activities are incorrectly handled in FPT_PHP.1. CC v2.1 indicates that FPT_PHP.1 is dependent on FMT_MOF.1. However, FPT_PHP.1 does not require user roles to be present in order to determine whether physical tampering has occurred, although a management function could be considered for such a role.

STATEMENT

FPT_PHP.1 is not dependent on FMT_MOF.1, although inclusion of the FPT_PHP.1 component in a PP or ST could require a management function for the user or role that determines whether physical tampering has occurred.

SPECIFIC INTERPRETATION

FPT_PHP.1 is relabeled as FPT_PHP.1-NIAP-0381. Unless otherwise noted in these changes, all normative and informative material associated with FPT_PHP.1 is incorporated unchanged into FPT_PHP.1-NIAP-0381, and all references to FPT_PHP.1 in the CC, CEM, or other Common Criteria documentation are changed to refer to FPT_PHP.1-NIAP-0381.

Within subclause 10.7, in the section "Management: FPT_PHP.1" replace paragraph 408 with:

The following actions could be considered for the management functions in FMT:

- a) management of the user or role that determines whether physical tampering has occurred.

In the component FPT_PHP.1, replace the text following "Dependencies:" with:

No dependencies

In Annex J.7, replace paragraph 1223 with: (additions shown thusly; deletions shown ~~thusly~~):

FPT_PHP.1 should be used when threats from unauthorised physical tampering with parts of the TOE are not countered by procedural methods. It addresses the threat of undetected physical tampering with the TSF. Typically, an authorised user would be given the function to verify whether tampering took place. As written, this component simply provides a TSF capability to detect tampering. ~~The dependency on~~ Specification of management functions in FMT_MOF.1 should be considered is required to specify who can make use of that capability, and how they can make use of that capability. If this function is realised by non-IT mechanisms (e.g. physical inspection) ~~it could be justified that the dependency on FMT_MOF.1 is not satisfied~~ management functions are not required.

SUPPORT:

This corrects the problem identified in the issue statement.