
I-0406: Automated Or Manual Recovery Is Acceptable

NUMBER: I-0406
STATUS: Posted for External Review
TYPE: NIAP Interpretation

TITLE: Automated Or Manual Recovery Is Acceptable
COMMENTS DUE BY: Monday, February 5, 2001 to IWG@gibraltar.ncsc.mil

SOURCE REFERENCE: CC v2.1 Part 2 Subclause 10.8 FPT_RCV
CC v2.1 Part 2 Subclause J.8 FPT_RCV

RELATED TO:
[I-0389](#) Recovery To A Known State

ISSUE:

The current CC v2.1 FPT_RCV.1 elements are worded in such a fashion as to preclude the use of automated mechanisms when manual recovery is to be supported. This is an unlikely situation; a PP/ST author may not care whether recovery is automated or manual.

STATEMENT OF INTERPRETATION:

Either manual or automated recovery systems are acceptable. The PP/ST author has the discretion to specify for what recovery scenarios automated recovery is appropriate, and for what recovery scenarios manual recovery is appropriate.

SPECIFIC INTERPRETATION:

To address this interpretation, the following changes are made to CC v2.1, Part 2: (additions marked thusly; deletions marked ~~thusly~~)

- In Clause 10.8, delete the existing FPT_RCV.1. As a result of this, Paragraph 415 and the "Management" section for FPT_RCV.1 are deleted; FPT_RCV.1 is removed from the "Audit" header between paragraphs 421 and 422, the "Component levelling" figure is modified to delete component 1, and the component decomposition figures (Clause 10, Figure 10.1 and Clause J, Figure J.1) showing the levelling structure for FPT are corrected to eliminate component 1. Additionally, the annex material for FPT_RCV.1 is deleted.
- FPT_RCV.2 is relabeled as FPT_RCV.2-NIAP-0406. Unless otherwise noted in these changes, all normative and informative material associated with FPT_RCV.2 is incorporated unchanged into FPT_RCV.2-NIAP-0406, and all references to FPT_RCV.2 in the CC, CEM, or other Common Criteria documentation is changed to refer to FPT_RCV.2-NIAP-0406.
- FPT_RCV.3 is relabeled as FPT_RCV.3-NIAP-0406. Unless otherwise noted in these changes, all normative and informative material associated with FPT_RCV.3 is incorporated unchanged into FPT_RCV.3-NIAP-0406, and all references to FPT_RCV.3 in the CC, CEM, or other Common Criteria documentation is changed to refer to FPT_RCV.3-NIAP-0406.
- The "Class Decomposition" figure in Clause 10, Figure 10.1 is modified to show component 2-NIAP-0406 as the first hierarchical component off of FPT_RCV, with component 3-NIAP-0406 immediately hierarchical to 2-NIAP-0406.
- The "Component Levelling" figure in Subclause 10.8 is modified to show component 2-NIAP-0406 as the first hierarchical component off of FPT_RCV, with component 3-NIAP-0406 immediately hierarchical to 2-NIAP-0406.

- Subclause 10.8, Paragraph 416 is replaced with the following:

~~FPT_RCV.2-NIAP-0406 Automated recovery~~ Recovery from Failure, provides, ~~for at least one type of service discontinuity, a specific list (possibly empty) of discontinuities for which the TSF must provide the capability for~~ recovery to a secure state without human intervention; recovery for other discontinuities may require human intervention.

- Subclause 10.8, Paragraph 417 is replaced with the following:

~~FPT_RCV.3-NIAP-0406 Automated recovery~~ Recovery without undue loss, also provides for ~~automated recovery from failure~~, but strengthens the requirements by disallowing undue loss of protected objects.

- In Clause 10.8, the following changes are made to FPT_RCV.2:

~~FPT_RCV.2-NIAP-0406 Automated recovery~~ Recovery from Failure

Hierarchical To: ~~FPT_RCV.1~~ No Other Components

~~FPT_RCV.2.21-NIAP-0406~~ For [selection: [assignment: *list of failures/service discontinuities*], "*no failures/service discontinuities*"], the TSF shall ensure the return of the TOE to a secure state using automated procedures.

~~FPT_RCV.2.42-NIAP-0406~~ When automated recovery from a failure or service discontinuity is not possible, the TSF shall enter a maintenance mode where the ability to return the TOE to a secure state is provided.

- In Clause 10.8, the following changes are made to FPT_RCV.3:

~~FPT_RCV.3-NIAP-0406 Automated recovery~~ Recovery without undue loss

Hierarchical To: ~~FPT_RCV.2-NIAP-0406~~

~~FPT_RCV.3.21-NIAP-0406~~ For [selection: [assignment: *list of failures/service discontinuities*], "*no failures/service discontinuities*"], the TSF shall ensure the return of the TOE to a secure state using automated procedures.

~~FPT_RCV.3.42-NIAP-0406~~ When automated recovery from a failure or service discontinuity is not possible, the TSF shall enter a maintenance mode where the ability to return the TOE to a secure state is provided.

- The "Class Decomposition" figure in Annex J, Figure J.1 is modified to show component 2-NIAP-0406 as the first hierarchical component off of FPT_RCV, with component 3-NIAP-0406 immediately hierarchical to 2-NIAP-0406.
- In Subclause J.8, the application notes for FPT_RCV.2 are modified as follows:

~~FPT_RCV.2-NIAP-0406 Automated recovery~~ Recovery from Failure

This component requires the TSF to provide mechanisms for automated or manual recovery. Automated recovery is considered to be more useful than manual recovery, as it allows the machine to operate in an unattended fashion. However, there may be situations where the list of discontinuities that required automated recovery is not known in advance, or the PP/ST author does not want to mandate automated recovery.

User Application Notes

~~The component FPT_RCV.2 extends the feature coverage of FPT_RCV.1 by requiring that there be at least one automated method of recovery from failure or service discontinuity. It addresses the threat of protection compromise resulting from an unattended TOE returning to an insecure state after recovery from a failure or other discontinuity.~~

FPT_RCV.2-NIAP-0406 addresses the threat of protection compromise resulting from a TOE returning to an insecure state after recover from a failure or other discontinuity. It provides the ability for unattended recovery for anticipated discontinuities.

Evaluator application notes

It is acceptable for the functions that are available to an authorised user for trusted recovery to be available only in a maintenance mode. Controls should be in place to limit access during maintenance to authorised users.

For FPT_RCV.2.12-NIAP-0406, it is the responsibility of the developer of the TSF to determine the set of recoverable failures and service discontinuities.

If "no failures/service discontinuities" is selected for FPT_RCV.2.1-NIAP-0406, this means that there are no explicitly mandated discontinuities for which automated recovery must be provided. The TOE developer always has the option to provide an automated recovery mechanism for a discontinuity.

It is assumed that the robustness of the automated recovery mechanisms will be verified.

Operations

Selection:

If there are no explicit situations for which automated recovery is mandated, "no failures/service discontinuities" should be selected in FPT_RCV.2.1-NIAP-0406. Otherwise, the assignment should be selected to provide the list of failures or other discontinuities for which automated recovery must be possible.

It is acceptable for a PP author complete only the selection and leave the assignment open, so as to indicate that the list of discontinuities for which automated recovery is required must be non-empty.

Assignment:

For FPT_RCV.2.21-NIAP-0406, the PP/ST author should specify the list of failures or other discontinuities for which automated recovery must be possible.

- In Subclause J.8, the application notes for FPT_RCV.3 are modified as follows:

FPT_RCV.3-NIAP-0406 ~~Automated recovery~~ Recovery without undue loss

This component requires the TSF to provide mechanisms for automated or manual recovery. Automated recovery is considered to be more useful than manual recovery, as it allows the machine to operate in an unattended fashion, but it runs the risk of losing a substantial number of objects. Preventing undue loss of objects provides additional utility to the recovery effort.

User Application Notes

The component FPT_RCV.3-NIAP-0406 extends the feature coverage of FPT_RCV.2-NIAP-0406 by requiring that there not be undue loss of TSF data or objects within the TSC. At FPT_RCV.2-NIAP-0406, the ~~automated~~ recovery mechanisms could conceivably recover by deleting all objects and returning the TSF to a known secure state. This type of drastic ~~automated~~ recovery is precluded in FPT_RCV.3-NIAP-0406.

This component addresses the threat of protection compromise resulting from an unattended TOE returning to an insecure state after recovery from a failure or other discontinuity with a large loss of TSF data or objects within the TSC.

Evaluator application notes

It is acceptable for the functions that are available to an authorised user for trusted recovery to be available only in a maintenance mode. Controls should be in place to limit access during maintenance to authorised users.

For FPT_RCV.3.1-NIAP-0406, it is the responsibility of the developer of the TSF to determine the set of recoverable failures and service discontinuities.

If "no failures/service discontinuities" is selected for FPT_RCV.3.1-NIAP-0406, this means that there are no explicitly mandated discontinuities for which automated recovery must be provided. The TOE developer always has the option to provide an automated recovery mechanism for a discontinuity.

It is assumed that the evaluators will verify the robustness of the automated recovery mechanisms.

Operations

Selection:

If there are no explicit situations for which automated recovery is mandated, "no failures/service discontinuities" should be selected in FPT_RCV.3.1-NIAP-0406. Otherwise, the assignment should be selected to provide the list of failures or other discontinuities for which automated recovery must be possible.

It is acceptable for a PP author complete only the selection and leave the assignment open, so as to indicate that the list of discontinuities for which automated recovery is required must be non-empty.

Assignment:

For FPT_RCV.3.1-NIAP-0406, the PP/ST author should specify the list of failures or other discontinuities for which automated recovery must be possible.

For FPT_RCV.3.3, the PP/ST author should provide a quantification for the amount of loss of TSF data or objects that is acceptable.

FURTHER CONSIDERATIONS:

Other families and components in Part 2 should be examined to correct any dependency references to components in FPT_RCV.

PROJECTED IMPACT:

Negligible impact anticipated.

SUPPORT:

This reworking of the FPT_RCV elements makes it so that automated mechanisms are permitted in all cases, or the PP/ST author has the option of indicating the specific situations in which automated recovery is mandated.