
I-0389: Recovery To A Known State

NUMBER: I-0389
STATUS: Ready to Send to Management/CCIMB
TYPE: NIAP Interpretation

TITLE: Recovery To A Known State

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-0406](#) Automated Or Manual Recovery Is Acceptable

ISSUE:

There are situations where some form of recovery from a known backup is required, but there is no formal model to argue that the known state is provably secure.

STATEMENT OF INTERPRETATION:

It must be possible to recover to a known previous state, as opposed to one that is provably secure.

SPECIFIC INTERPRETATION:

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

- The following component is added to the FPT_RCV family in Subclause 10.8. This component would be immediately below the current lowest component in the existing FPT_RCV hierarchy:

FPT_RCV.NIAP-0389-1 Recovery to Known State

Hierarchical to: No other components.

FPT_RCV.NIAP-0389-1.1 For [selection: [assignment: *list of failures/service discontinuities*], "*no failures/service discontinuities*"], the TSF shall ensure the return of the TOE to a previously known state using automated procedures.

FPT_RCV.NIAP-0389-1.2 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 previously known state is provided.

Dependencies:

AGD_ADM.1 Administrator guidance

- In Subclause 10.8, rework the component levellings to make FPT_RCV.2-NIAP-0406 immediately hierarchical to the new component.
- In Clause 10, Figure 10.1, the class decomposition figure is updated to show that component 2-NIAP-0406 is immediately hierarchical to component NIAP-0389-1.
- In Subclause 10.8, add the following after the "Component Levelling" diagram:

FPT_RCV.NIAP-0389-1 Recovery to a Known State, allows a TOE to only provide mechanisms that involve human intervention to a previously known, but not provably secure, state.

- In Subclause 10.8, FPT_RCV.2-NIAP-0406, change the "Hierarchical To:" as follows:

Hierarchical To: ~~No other components~~ FPT_RCV.NIAP-0389-1

- In Subclause J.8, add the following after paragraph 1236:

FPT_RCV.NIAP-0389-1 Recovery to a Known State

In the hierarchy of the trusted recovery family, recovery that recovers only to a previously known state, as opposed to known secure state, is the least desirable.

User Application Notes

This component is intended for use in TOEs that do not require recovery to a known secure state. The requirements of this component reduce the threat of protection compromise resulting from an attended TOE returning to an unknown state after recovery from a failure or other discontinuity.

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.

If "no failures/service discontinuities" is selected for FPT_RCV.NIAP-0389.1, 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.

Operations

Selection:

If there are no explicit situations for which automated recovery is mandated, "no failures/service discontinuities" should be selected in FPT_RCV.NIAP-0389-1.1. 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 to 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.NIAP-0389-1.1, the PP/ST author should specify the list of failures or other discontinuities for which automated recovery must be possible.

- In Annex J, Figure J.1, the class decomposition figure is updated to show that component 2-NIAP-0406 is immediately hierarchical to component NIAP-0389-1.

PROJECTED IMPACT:

Negligible impact anticipated.

SUPPORT:

The words in the annex for FPT_RCV state:

Throughout this family, the phrase "secure state" is used. This refers to some state in which the TOE has consistent TSF data and a TSF that can correctly enforce the policy. This state may be the initial "boot" of a clean system, or it might be some checkpointed state. The "secure state" is defined in the TSP model. If the developer provided a clear definition of the secure state and the reason why it should be considered secure, the dependency from FPT_FLS.1 to ADV_SPM.1 can be argued away.

Although this allows a secure state to be a previously checkpointed state, this ability is buried. This component makes it explicit; it also makes it clear that a previously known state may or may not be a secure state.

Note: This interpretation is being applied to the CC as modified by I-0406.