
I-0356: FDP_RIP Annex: Reuse Of Subject Data Notes

TYPE: NIAP Interpretation
NUMBER: I-0356
STATUS: Ready for External Repost after Interpretations Board Rework/Review

TITLE: FDP_RIP Annex: Reuse Of Subject Data Notes
COMMENTS DUE BY: Monday, February 25, 2002 to ccevs-cmt@nist.gov

SOURCE REFERENCE: CC v2.1 Part 2 Subclause F.9 FDP_RIP
CC v2.1 Part 2 Subclause J.11 FPT_SEP

RELATED TO:
[I-0350](#) Clarification Of Resources/Objects For Residual Information Protectio

ISSUE:

TSF internal data structures have, at times, been considered as a factor contributing to residual data problems. Some products have had residual data problems because, even though they cleared shared objects and the subject's address space at creation, the TSF, as part of its execution of a subject, moved data left over from a previous subject in a TSF internal data structure to a shared object or another subject's address space. The potential for violation of the TSP that arises from such TSF use of internal data structures needs to be addressed in the CC.

STATEMENT

Reuse of resources that are serially reused by different subjects during execution of those subjects is more properly covered as part of the elements requiring subject separation (FPT_SEP), as opposed to residual information protection.

SPECIFIC INTERPRETATION

To address this interpretation, the following changes are made to CC v2.1, Part 2:

- In Annex F.9, delete the second paragraph (paragraph number 889) under User notes.
- After paragraph 1266 in Annex J.11, insert the following new second paragraph under User notes:

FPT_SEP provides that the security domains of subjects must be separate. This implies that no information from one subject must be permitted to flow to another subject except through explicit TSF-mediated interchanges. Hence, FPT_SEP is actually stronger than FDP_RIP in that it covers not only reuse through allocation/deallocation, but reuse of data structures as part of task scheduling and other TSF internal operations. It also covers internal data structures, and situations where subject creation and destruction is static or controlled by the TSF, and cannot be performed upon explicit subject request.

SUPPORT:

TSF internal data structures have, at times, been considered as a factor contributing to residual data problems. Some products have had residual data problems because, even though they cleared shared objects and the subject's address space at creation, the TSF, as part of its execution of a subject, moved data left over from a previous subject in a TSF internal data structure to a shared object or another subject's address space.

The TSF is responsible for the prevention of inadvertent information transfer between subjects that result from operations internal to it. The results of such operations are not normally visible to subjects under the control of the TSF. If such

operations result from a subject's allocation or deallocation request for an object, they fall under the residual information protection family; if they are not directly visible to the subject, they are considered under the domain separation family.