
I-0464: Conditional Requirements

TYPE: Request for Interpretation
NUMBER: I-0464
STATUS: Ready for External Repest after Interpretations Board
Rework/Review

TITLE: Conditional Requirements

FIRST POST: [\[cc-cmt 00553\]](#)
MOST RECENT REPOST: [\[cc-cmt 00720\]](#)
COMMENTS DUE BY: Friday, February 6, 2004 to cc-cmt@nist.gov

RELATED TO: <None>

ISSUE:

Currently, the CC does not provide the ability to specify conditional requirements, i.e., requirements that only need to be met under a particular condition. This would be useful flexibility for protection profiles, which might be used in differing but similar environments.

PROPOSED RESOLUTION

A future version of the Common Criteria should support the notion of conditional components as a form of operation.

SPECIFIC RESOLUTION

To address this interpretation, it is suggested that a new operation be added to the Common Criteria, conditionals, that operate at the component level. This would take the form:

CONDITION: [statement of conditions]

Conditions would be an operation similar to iteration; that is: they would need to be clearly identified as conditional, and would operate at the level of a full component.

For any components in a PP that are expressed using the conditional operator, the CEM would need to require the evaluator to verify the following during a PP evaluation:

- That the objective mapped to the component is subject to equal conditions, or is sufficiently general for the component to apply.
- That the threat mapped to the component through the objective is subject to equal conditions, or there are sufficient alternative components so as to cover the stated threat.
- That for a given condition, the set of applicable components does not create conflicting components, internal inconsistencies, or unsatisfied dependencies.

The application of a condition would need to be clearly indicated in an ST. This could be done through a distinct section that identifies the conditional components included and excluded, and the rationale therefore.

Conditional components would only be valid in a protection profile. All conditional statements must be resolved by the time they are expressed in a security target.

SUPPORT:

When writing a general specification, for example, a Protection Profile, it is often unknown the specific protocols or approaches that will be taken in the eventual implementation. For example:

- Any of a variety of cryptographic protocols might be acceptable, but depending on the protocol chosen, there might be specific standards or behavior characteristics that must be met.
- Either pre- or post- selection of audit events may be acceptable.
- There might be different components to address different authentication mechanisms, but the overall threat and objective is the same.

However, CC v2.1 does not support the notion of condition components. The closest it comes to having them is the AUDIT sections, which suggest audit requirements to be included. It also supports iteration on components, which allow for different components to have different scopes. Conditional components are similar, in that they affect the scope (although that scope is determined as a profile is included into a target, instead of at the time of the writing of the profile)

This proposal suggests that conditional component be treated as yet another form of operation. Hence, conditional components would only be valid in a protection profile. All conditional statements must be resolved by the time they are expressed in a security target.

The following is an example of the use of the conditional operation to provide for pre- or post- audit selection:

FAU_SEL.1: Selective Audit

CONDITION: ST does not include FAU_SAR.3

(text of FAU_SEL.1)

FAU_SAR.3: Selectable Audit Review

CONDITION: ST does not include FAU_SEL.1

(text of FAU_SAR.3)