
I-0440: Clarification Of Detection/Prevention For FIA_UAU.3

TYPE: Guidance
NUMBER: I-0440
STATUS: Ready for External Review

TITLE: Clarification Of Detection/Prevention For FIA_UAU.3
COMMENTS DUE BY: Friday, February 6, 2004 to cc-cmt@nist.gov

SOURCE REFERENCE: CC v2.1 Part 2 Subclause 7.4 FIA_UAU.3
CC v2.1 Part 2 Subclause G.4 FIA_UAU.3

RELATED TO: <None>

ISSUE:

The text of FIA_UAU.3 appears to permit the use of fraudulent data, which can occur if "detect" is the only option chosen. An additional problem is that there are two possible interpretations of "detect": detect an attempt to subvert, or detect the subversion itself.

STATEMENT

The concern arises from a misunderstanding of the requirement. The Annex makes clear the following cases (note that this component applies only to generated non-sharable data, such as biometric data, as opposed to sharable data such as passwords):

- Detecting the use of copied data (and by implication, not preventing its use).
- Preventing the acceptance of copied or fraudulent data, through an implementation that simply makes such data unacceptable.
- Performing both actions, i.e., detecting attempts to use copied or fraudulent data and not accepting such data as valid authentication.

SUPPORT:

The wording in the main body of the CC with respect to this component is very concise, just using the terms "detect" and "prevent". The Annex provides useful clarification, but it is also not as clear as it could be.

The key assumption for this component is that the data is not normally sharable by out of band channels. One can share passwords out of band; one cannot share the bits that encapsulate a fingerprint. So how does one deal with the threat from digitally copied or forged authentication data.

In the first case, "detect", one can implement mechanism to detect its use, but there might not be the need or ability to prevent its use. This might be done in an intrusion detection system.

In the second case, "prevent", one might design an implementation that simply made the authentication data unusable except by the correct party. There would be no need for detection, as the data would be treated as any other invalid authentication.

In the last case, "detect and prevent", both mechanisms would come into play. The TSF would be able to detect the use of such data (and report it, if auditing was in place). It would also be able to reject such data as an invalid authentication.