Australian Government
Department of Defence

Defence Signals Directorate

Australasian Information Security Evaluation Program

Analysis and testing for insecure states (AVA_MSU.3) - CC V2.2

Common Evaluation Methodology

10 February 2006

Version 1.1

Amendment Record

Version	Date	Description
1.0	1 February 2006	Released.
1.1	10 February 2006	Releasable to AISEFs.

Table of Contents

1 Analysis and testing for insecure states

1.1 Objectives

1 The objective of this sub-activity is to ensure that misleading, unreasonable and conflicting guidance is absent from the guidance documentation, and that secure procedures for all modes of operation have been addressed. Insecure states should be easy to detect. In this component, an analysis of the guidance documentation by the developer is required to provide additional assurance that the objective has been met, and this analysis is validated and confirmed through testing by the evaluator.

1.2 Input

2 The evaluation evidence for this sub-activity is:

a) the ST;

b) the functional specification;

c) the high-level design;

d) the low-level design;

e) the subset of the implementation representation;

f) the TOE security policy model;

g) the user guidance;

h) the administrator guidance;

i) the secure installation, generation, and start-up procedures;

j) the misuse analysis of the guidance;

k) the test documentation;

l) the TOE suitable for testing.

1.3 Evaluator Actions

1.3.1 AVA_MSU.3.1E

AVA_MSU.3.1C The guidance documentation shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AVA_MSU.3-1 The evaluator ***shall examine*** the guidance and other evaluation evidence to determine that the guidance identifies all possible modes of operation of the TOE (including, if applicable, operation following failure or operational error), their consequences and implications for maintaining secure operation.

3 Other evaluation evidence, particularly the functional specification and test documentation, provide an information source that the evaluator should use to determine that the guidance contains sufficient guidance information.

4 The evaluator should focus on a single security function at a time, comparing the guidance for securely using the security function with other evaluation evidence, to determine that the guidance related to the security function is sufficient for the secure usage (i.e consistent with the TSP) of that security function. The evaluator should also consider the relationships between functions, searching for potential conflicts.

AVA_MSU.3.2C The guidance documentation shall be complete, clear, consistent and reasonable.

AVA_MSU.3-2 The evaluator ***shall examine*** the guidance to determine that it is clear and internally consistent.

5 The guidance is unclear if it can reasonably be misconstrued by an administrator or user, and used in a way detrimental to the TOE, or to the security provided by the TOE.

6 For guidance on consistency analysis see B.3.

AVA_MSU.3-3 The evaluator ***shall examine*** the guidance and other evaluation evidence to determine that the guidance is complete and reasonable.

7 The evaluator should apply familiarity with the TOE gained from performing other evaluation activities to determine that the guidance is complete.

8 In particular, the evaluator should consider the functional specification and TOE summary specification. All security functions described in these documents should be described in the guidance as required to permit their secure administration and use. The evaluator may, as an aid, prepare an informal mapping between the guidance and these documents. Any omissions in this mapping may indicate incompleteness.

9 The guidance is unreasonable if it makes demands on the TOE's usage or operational environment that are inconsistent with the ST or unduly onerous to maintain security.

10 The evaluator should note that results gained during the performance of work units from the AGD_ADM sub-activity will provide useful input to this examination.

AVA_MSU.3.3C The guidance documentation shall list all assumptions about the intended environment.

AVA_MSU.3-4 The evaluator ***shall examine*** the guidance to determine that all assumptions about the intended environment are articulated.

11 The evaluator analyses the assumptions about the intended TOE security environment of the ST and compares them with the guidance to ensure that all assumptions about the intended TOE security environment of the ST that are relevant to the administrator or user are described appropriately in the guidance.

AVA_MSU.3.4C The guidance documentation shall list all requirements for external security measures (including external procedural, physical and personnel controls).

AVA_MSU.3-5 The evaluator ***shall examine*** the guidance to determine that all requirements for external security measures are articulated.

12 The evaluator analyses the guidance to ensure that it lists all external procedural, physical, personnel and connectivity controls. The security objectives in the ST for the non-IT environment will indicate what is required.

AVA_MSU.3.5C The analysis documentation shall demonstrate that the guidance documentation is complete.

AVA_MSU.3-6 The evaluator ***shall examine*** the developer's analysis to determine that the developer has taken adequate measures to ensure that the guidance is complete.

13 The developer analysis may comprise mappings from the ST or the functional specification to the guidance in order to demonstrate that the guidance is complete. Whatever evidence is provided by the developer to demonstrate completeness, the evaluator should assess the developer's analysis against any deficiencies found during the conduct of work units AVA_MSU.3-1 through AVA_MSU.3-5, and AVA_MSU.3-7.

1.3.2 AVA_MSU.3.2E

> **AVA_MSU.3.2E** The evaluator shall repeat all configuration and installation procedures, and other procedures selectively, to confirm that the TOE can be configured and used securely using only the supplied guidance documentation.

AVA_MSU.3-7 The evaluator ***shall perform*** all administrator and user (if applicable) procedures necessary to configure and install the TOE to determine that the TOE can be configured and used securely using only the supplied guidance.

14 Configuration and installation requires the evaluator to advance the TOE from a deliverable state to the state in which it is operational and enforcing a TSP consistent with the security objectives specified in the ST.

15 The evaluator should follow only the developer's procedures as documented in the user and administrator guidance that is normally supplied to the consumer of the TOE. Any difficulties encountered during such an exercise may be indicative of incomplete, unclear, inconsistent or unreasonable guidance.

16 Note that work performed to satisfy this work unit may also contribute towards satisfying evaluator action ADO_IGS.1.2E.

AVA_MSU.3-8 The evaluator ***shall perform*** other security relevant procedures specified in the guidance to determine that the TOE can be configured and used securely using only supplied guidance.

17 The evaluator should follow only the developer's procedures as documented in the user and administrator guidance that is normally supplied to the consumer of the TOE.

18 The evaluator should employ sampling in carrying out this work unit. When choosing a sample the evaluator should consider:

a) the clarity of the guidance - any potential unclear guidance should be included in the sample;

b) guidance that will be used most often - infrequently used guidance should not normally be included in the sample;

c) complexity of the guidance - complex guidance should be included in the sample;

d) severity of error - procedures for which error imparts the greatest severity on security should be included in the sample;

e) the nature of the TOE - the guidance related to the normal or most likely use of the TOE should be included in the sample.

19 For guidance on sampling see B.2

1.3.3 AVA_MSU.3.3E

AVA_MSU.3.3E The evaluator shall determine that the use of the guidance documentation allows all insecure states to be detected.

AVA_MSU.3-9 The evaluator ***shall examine*** the guidance to determine that sufficient guidance is provided for the consumer to effectively administer and use the TOE's security functions, and to detect insecure states.

20 TOEs may use a variety of ways to assist the consumer in effectively using the TOE securely. One TOE may employ functionality (features) to alert the consumer when the TOE is in an insecure state, whilst other TOEs may be delivered with enhanced guidance containing suggestions, hints, procedures, etc. on using the existing security features most effectively; for instance, guidance on using the audit feature as an aid for detecting insecure states.

21 To arrive at a verdict for this work unit, the evaluator considers the TOE's functionality, its purpose and intended environment, and assumptions about its usage or users. The evaluator should arrive at the conclusion that, if the TOE can transition into an insecure state, there is reasonable expectation that use of the guidance would permit the insecure state to be detected in a timely manner. The potential for the TOE to enter into insecure states may be determined using the evaluation deliverables, such as the ST, the functional specification and the high-level design of the TSF.

1.3.4 AVA_MSU.3.4E

AVA_MSU.3.4E The evaluator shall confirm that the analysis documentation shows that guidance is provided for secure operation in all modes of operation of the TOE.

AVA_MSU.3-10 The evaluator ***shall examine*** the developer's analysis of the guidance to determine that guidance is provided for secure operation in all modes of operation of the TOE.

22 The results of evaluation action AVA_MSU.3.1E should provide a basis with which to evaluate the developer's analysis. Having evaluated the potential for misuse of the guidance, the evaluator should be able to determine that the developer's misuse analysis meets the objectives of this sub-activity.

1.3.5 AVA_MSU.3.5E

AVA_MSU.3.5E The evaluator shall perform independent testing to determine that an administrator or user, with an understanding of the guidance documentation, would reasonably be able to determine if the TOE is configured and operating in a manner that is insecure.

AVA_MSU.3-11 The evaluator ***shall devise*** independent misuse tests based on the guidance documentation to determine, whether an administrator or user will be able to detect if the TOE is configured and operating in a manner that is insecure.

23 The evaluator frames test cases and testing strategy being appropriate for the TOE.

24 With an understanding of the expected behaviour of the TOE under a concrete configuration the evaluator has to determine the most feasible way to test for the TOE’s misuse. All TOE configurations and modes of operation being part of the evaluation have to be considered, but sampling of misuse testing is allowed. The most critical aspects have to be covered. In case of a sampling, a rationale has to be provided.

AVA_MSU.3-12 The evaluator ***shall produce*** misuse test documentation for the misuse test subset in sufficient details to enable the tests to be repeatable.

25 The test documentation shall include:

a) an exact identification of the TOE configuration and the mode of operation being under test;

b) an unambiguous identification of the relevant guidance documentation for the specific test;

c) instructions for observing the behaviour of the TSF and for determining a secure or insecure state of the TOE;

d) information on what the expected secure or insecure state of the TOE is.

26 The intent of specifying this level of detail in the test documentation is to allow another evaluator to repeat the tests and obtain an equivalent result.

AVA_MSU.3-13 The evaluator ***shall conduct*** independent misuse testing.

27 The evaluator uses the misuse test documentation resulting from the previous work unit as a basis for executing independent misuse tests on the TOE.

AVA_MSU.3-14 The evaluator ***shall record*** the actual results of the misuse tests.

28 While some specific details of the actual test results may be different from those expected the overall result should be identical. Any differences in terms of insecure states of the TOE should be justified.

29 In case of an identified insecure state of the TOE, consequences for guidance documentation or TOE design have to be determined in order to enforce that an administrator or user, with an understanding of the guidance documentation, will reasonably be able to determine if the TOE is configured and operating in a manner that is insecure.