Australian Government
Department of Defence

Defence Signals Directorate

Australasian Information Security Evaluation Program

Security Policy Model (ADV_SPM.3) - CC V2.2

Common Evaluation Methodology

15 February 2006

Version 1.2

Amendment Record

Version	Date	Description
1.0	30 June 2005	Released.
1.1	15 August 2005	Released to AISEFs.
1.2	15 February 2006	Added CC V2.2 to title.

Table of Contents

1 Formal TOE Security Policy Model (ADV_SPM.3)

1.1 Objectives

1 The objectives of this sub-activity are to determine whether the security policy model clearly and consistently describes the rules and characteristics of the security policies and whether this description corresponds with the description of security functions in the functional specification.

1.2 Input

2 The evaluation evidence for this sub-activity is:

a) the ST;

b) the functional specification;

c) the TOE security policy model;

d) the user guidance;

e) the administrator guidance.

1.3 Evaluator Actions

1.3.1 ADV_SPM.3.1E

ADV_SPM.3.1C	The TSP model shall be ***formal***.

ADV_SPM.3-1 The evaluator ***shall examine*** the security policy model to determine that it describes the TSP model using a formal style.

3 The purpose of the formal security policy model is to define security (in the context of the TOE and its environment) in a clear, abstract way, independent of the TOE implementation. Whilst the formal security policy model may be complex, and require considerable effort to understand, once understood it should clearly be the correct definition of security for the TOE.

4 The formal security model is to be specified using an appropriate formal notation agreed by the Scheme.

ADV_SPM.3-2 The evaluator ***shall examine*** the security policy model to determine that the formal notations are supported by syntactic and semantic rules.

5 The notation should possess well defined syntax and semantics, with both being themselves expressed in formal notations which satisfy either of the first two criteria. Syntactic and Semantic rules define how to recognise constructs unambiguously and determine their meaning.

ADV_SPM.3-3 The evaluator ***shall examine*** the security policy model to determine that it contains all necessary informal explanatory text.

6 Supporting narrative descriptions are necessary for those portions of the model that are difficult to understand only from formal description.

ADV_SPM.3.2C The TSP model shall describe the rules and characteristics of all policies of the TSP that can be modeled.

ADV_SPM.3-4 The evaluator ***shall check*** the model to determine that all security policies that are explicitly included in the ST are modeled.

7 The security policy is expressed by the collection of the functional security requirements in the ST. Therefore, to determine the nature of the security policy (and hence what policies must be modeled), the evaluator analyses the ST functional requirements for those policies explicitly called for (by Access control policy (FDP_ACC) and Information flow control policy (FDP_IFC), if included in the ST).

8 If the ST contains no explicit policies (because neither Access control policy (FDP_ACC) nor Information flow control policy (FDP_IFC) are included in the ST), this work unit is not applicable and is therefore considered to be satisfied.

ADV_SPM.3-5 The evaluator ***shall examine*** the model to determine that all security policies represented by the security functional requirements claimed in the ST are modeled.

9 In addition to the explicitly-listed policies (see work unit ADV_SPM.1-2), the evaluator analyses the ST functional requirements for those policies implied by the other functional security requirement classes. For example, inclusion of FDP: User data protection requirements (other than Access control policy (FDP_ACC) and Information flow control policy (FDP_IFC)) would need a description of the Data Protection policy being enforced; inclusion of any FIA: Identification and authentication requirements would necessitate that a description of the Identification and Authentication policies be present in the model; inclusion of FAU: Security audit requirements need a description of the Audit policies; etc. While the other functional requirement families are not typically associated with what are commonly referred to as security policies, they nevertheless do enforce security policies (e.g. non-repudiation, reference mediation, privacy, etc.) that must be included in the security policy model.

10 If the ST contains no such implicit policies, this work unit is not applicable and is therefore considered to be satisfied.

ADV_SPM.3-6 The evaluator ***shall examine*** the rules and characteristics of the model to determine that the modeled security behaviour of the TOE is clearly articulated.

11 The rules and characteristics describe the security posture of the TOE. It is likely that such a description would be contained within an evaluated and certified ST. In order to be considered a clear articulation, such a description should define the notion of security for the TOE, identify the security attributes of the entities controlled by the TOE and identify the TOE actions which change those attributes. For example, if a policy attempts to address data integrity concerns, the policy model would:

a) define the notion of integrity for that TOE;

b) identify the types of data for which the TOE would maintain integrity;

c) identify the entities that could modify that data;

d) identify the rules that potential modifiers must follow to modify data.

ADV_SPM.3.3C The TSP model shall include a rationale that demonstrates that it is consistent and complete with respect to all policies of the TSP that can be modeled.

ADV_SPM.3-7 The evaluator ***shall examine*** the model rationale to determine that the behaviour modeled is consistent with respect to policies described by the security polices (as articulated by the functional requirements in the ST).

12 In determining consistency, the evaluator verifies that the rationale shows that each rule or characteristic description in the model accurately reflects the intent of the security policies. For example, if a policy stated that access control was necessary to the granularity of a single individual, then a model describing the security behaviour of a TOE in the context of controlling groups of users would not be consistent. Likewise, if the policy stated that access control for groups of users was necessary, then a model describing the security behaviour of a TOE in the context of controlling individual users would also not be consistent.

13 Assurance is to be gained from an explicit and general statement of the policies underlying the TOE security functional requirements. The assurance gained is two-fold: collecting the description of each security policy into a concise whole aids in understanding the details of the policies being enforced. Additionally, such a collected description makes it much easier to see any gaps or inconsistencies (which must be sought as part of the Security policy modeling (ADV_SPM).*.3C element), and provides a clear characterisation of secure states (sought as part of the Security policy modeling (ADV_SPM).*.2C element).

14 For guidance on consistency analysis see B.3.

ADV_SPM.3-8 The evaluator ***shall examine*** the model rationale to determine that the behaviour modeled is complete with respect to the policies described by the security policies (i.e. as articulated by the functional requirements in the ST).

15 In determining completeness of this rationale, the evaluator considers the rules and characteristics of the model and map those rules and characteristics to explicit policy statements (i.e. functional requirements). The rationale should show that all policies that are required to be modeled have an associated rule or characteristic description in the model.

ADV_SPM.3.4C The demonstration of correspondence between the TSP model and the functional specification shall show that all of the security functions in the functional specification are consistent and complete with respect to the TSP model.

ADV_SPM.3-9 The evaluator ***shall examine*** the functional specification correspondence demonstration of the policy model to determine that it identifies all security functions described in the functional specification that implement a portion of the policy.

16 In determining completeness, the evaluator reviews the functional specification, identifies which functions directly support the model and verifies that these functions are present in the functional specification correspondence demonstration of the model.

ADV_SPM.3-10 The evaluator ***shall examine*** the functional specification correspondence demonstration of the model to determine that the descriptions of the functions identified as implementing the model are consistent with the descriptions in the functional specification.

17 To demonstrate consistency, the evaluator verifies that the functional specification correspondence shows that the functional description in the functional specification of the functions identified as implementing the policy described in the model identify the same attributes and characteristics of the model and enforce the same rules as the model.

18 In cases where a security policy is enforced differently for untrusted users and administrators, the policies for each are described consistently with the respective behaviour descriptions in the user and administrator guidance. For example, the "identification and authentication" policy enforced upon remote untrusted users might be more stringent than that enforced upon administrators whose only point of access is within a physically-protected area; the differences in authentication should correspond to the differences in the descriptions of authentication within the user and administrator guidance.

19 For guidance on consistency analysis see CEM B.3.

ADV_SPM.3.5C ***Where the functional specification is semiformal, the demonstration of correspondence between the TSP model and the functional specification shall be semiformal.***

ADV_SPM.3-11 Where the functional specification is semiformal, the evaluator ***shall examine*** the security policy model to determine that the demonstration of correspondence between the TSP model and the functional specification is presented using a semiformal approach.

20 Where the functional specification is not semiformal, this work unit is not applicable.

21 A semiformal demonstration of correspondence requires a structured approach to the analysis of correspondence. This approach should lessen ambiguity that could exist in an informal correspondence by limiting the interpretation of the terms included in the correspondence. Pointers and references to other documents may be used.

22 The evaluator performs ADV_SPM.3-9 and ADV_SPM.3-10 within the context of the semiformal demonstration.

ADV_SPM.3.6C ***Where the functional specification is formal, the proof of correspondence between the TSP model and the functional specification shall be formal.***

ADV_SPM.3-12 The evaluator ***shall check*** that a formal proof of correspondence between the security policy model and the functional specification has been provided.

23 Where the functional specification is not formal, this work unit is not applicable.

24 A formal proof of correspondence uses well-established mathematical concepts to define the syntax and semantics of the formal notation and the proof rules that support logical reasoning.

25 A TOE may not uphold the security policy model unless the correspondence between the security policy model and functional specification is proven.

26 Where the formal functional specification and the formal security policy model are not specified in the same formal language, the evaluator should confirm that a translation between the formal notations has been provided. The evaluator should examine that this translation is correct.

ADV_SPM.3-13 The evaluator ***shall examine*** the proof of the correspondence between the security policy model and the functional specification is correct and complete.

27 The evaluator confirms that the formal functional specification is shown to be deducible from the axioms of the formal security policy model and that the formal functional specification does not conflict with the formal security policy model.

28 Evaluators should consider the following questions when examining the formal proof:

a) Is the objective of the proof appropriate?

b) Is the formalisation of the objective of the proof correct?

c) Are the assumptions or axioms from which the proof begins correct?

d) Are the deductive steps correct?

29 The evaluator performs ADV_SPM.3-9 and ADV_SPM.3-10 within the context of the formal demonstration.