Australian Government
Department of Defence

Defence Signals Directorate

Australasian Information Security Evaluation Program

Covert Channel Analysis (AVA_CCA.2) - CC V2.2

Common Evaluation Methodology

10 February 2006

Version 1.1

Amendment Record

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

Table of Contents

1 Systematic covert channel analysis (AVA_CCA.2)

1.1 Objectives

1 The objective of this sub-activity is to verify that the developer has identified covert channels through a systematic search.

1.2 Application Notes

2 The application of covert channel analysis techniques requires specialist knowledge. Developer representatives producing covert channel analyses deliverables should have an intimate knowledge of the TOE and have experience in the application of covert channel analysis techniques.

3 Evaluators must have expertise in the area of covert channel analysis in order to perform several work units in this activity.

1.3 Input

4 The evaluation evidence for this sub-activity is:

a) the ST;

b) the Functional Specification;

c) the Implementation Representation;

d) the Security Policy Model;

e) the Administrator Guidance;

f) the User Guidance.

1.4 Evaluator Actions

1.4.1 AVA_CCA.2.1E

AVA_CCA.2.1C The analysis documentation shall identify covert channels and estimate their capacity.

AVA_CCA.2-1 The evaluator ***shall examine*** the analysis documentation to determine that it identifies any covert channels discovered by the developer.

5 The covert channels may be partitioned into storage channels and timing channels. If no covert channels are identified, the design principles that prevented them should be documented and justified so as to convince the evaluator that the result is valid.

AVA_CCA.2-2 The evaluator ***shall check*** that each identified covert channel has an estimated channel capacity.

6 The capacity of a channel is its maximum possible error-free information rate in bits per second.

AVA_CCA.2.2C The analysis documentation shall describe the procedures used for determining the existence of covert channels, and the information needed to carry out the covert channel analysis.

AVA_CCA.2-3 The evaluator ***shall examine*** the analysis documentation to determine that it describes the procedures used for determining the existence of covert channels.

7 The search for covert channels may be performed using various methods. These include manual methods such as the shared resource matrix, or through the use of automated tools based on information flow formulas, covert flow trees, or possibly other techniques. The techniques employed for the search for covert channels may depend on the type and operational environment of the TOE.

8 The evaluator determines that the procedures provide sufficient detail to allow the developer’s search for covert channels to be repeated providing consistent results.

AVA_CCA.2-4 The evaluator ***shall examine*** the analysis documentation to determine that it includes a description of the information needed to carry out the covert channel analysis.

9 Covert channel analysis may be performed using various design representations, ranging from abstract models through to machine code and hardware representations.

10 The evaluator examines the evidence to determine that the information used to perform the covert channel analysis includes, as a minimum, the functional specification and the implementation representation.

11 The evaluator determines wether sufficient information has been considered in performing the covert channel analysis. For example, any system resource that is shared between processes operating at different security levels could be exploitable as a covert channel. The covert channel analysis must consider details of all such interactions, which may require an analysis of hardware as well as software.

AVA_CCA.2.3C The analysis documentation shall describe all assumptions made during the covert channel analysis.

AVA_CCA.2-5 The evaluator ***shall examine*** the analysis documentation to determine that all assumptions supporting the analysis are articulated.

12 The evaluator searches for areas of developer analysis that leave any variable affecting the analysis undefined. For example, where a covert channel capacity estimate is provided, assumptions regarding transmission error probabilities shall be explicitly stated.

AVA_CCA.2-6 The evaluator ***shall examine*** the analysis documentation to determine that all assumptions supporting the analysis are valid.

13 For example, an assumption regarding transmission errors based on the highest probability error rate would be flawed if the objective of the analysis that the assumption supports is to calculate the maximum obtainable capacity of a given covert channel. In this circumstance, transmission error assumptions must be based on the lowest noise or error rate.

14 Assumptions supporting the analysis should reflect the worst case, unless the worst case is invalidated by the ST. Where a number of different possible scenarios exist, and these are dependent on the behaviour of the human user or attacker, the case that represents the highest covert channel capacity / worst case exploitation scenario should be assumed unless, as previously stated, this case is invalid.

AVA_CCA.2.4C The analysis documentation shall describe the method used for estimating channel capacity, based on worst case scenarios.

AVA_CCA.2-7 The evaluator ***shall examine*** the analysis documentation to determine that the method used for estimating channel capacity has been fully described.

15 The capacity of a channel is its maximum possible error-free information rate in bits per second. It is a function of the following factors:

a) The quantity of information that can be transmitted per execution of a covert channel scenario;

b) The time required to exercise the scenario;

c) The effect of other system activities on the rate of the transfer (e.g. workload of the system etc.).

16 The evaluator ensures that the assumed or actual system specifications are recorded, including:

a) the speed of system components;

b) the system configuration;

c) the sizes of memory and cache components;

d) the system initialization.

17 The sensitivity of the estimation results to configuration changes should also be recorded. All channel estimations must be repeatable based on the recorded information.

AVA_CCA.2-8 The evaluator ***shall examine*** the analysis documentation to determine that the method used for estimating channel capacity has been based on worst case scenarios.

18 Basing channel capacity on worst case scenarios is achieved by assuming the highest information transfer rate given the above factors. For example, assuming the lowest possible transmission error rate and that the effect of other system activities is negligible.

AVA_CCA.2.5C The analysis documentation shall describe the worst case exploitation scenario for each identified covert channel.

AVA_CCA.2-9 The evaluator ***shall examine*** the analysis documentation to determine that the worst case exploitation scenario is described for each identified covert channel.

19 For a covert channel to be exploited, it is necessary to find a scenario that allows the transfer of information between two user processes that would not be allowed to communicate directly under the TOE's security policy.

20 In describing an exploitation scenario, the developer defines the sequence of system operations that allows a sending process to modify a TOE resource attribute in violation of the TOE security policy and allows a receiving process to detect the modification.

21 The exploitation scenario should answer the following:

a) Is the covert channel exploitable in the TOE's intended environment?

b) What type of data is transferred through the covert channel (e.g. TSF data, user data)?

c) What is the exploitable channel capacity, giving consideration to error correction, communication negotiation, or other factors?

22 The worst case scenario assumes the worst case for all factors affecting the severity of the security policy violation caused by the covert channel.

AVA_CCA.2.6C The analysis documentation shall provide evidence that the method used to identify covert channels is systematic.

AVA_CCA.2-10 The evaluator ***shall examine*** the analysis documentation to determine that the search for covert channels is shown to be performed in accordance with a systematic methodology.

23 Examples of systematic covert channel search methodologies include the shared resource matrix, information flow formulas, and covert flow trees. The evaluator determines wether the evidence shows that the methodology is structured in its approach, uses defined processes to identify covert channels, and is proven (e.g. by widespread use, or by specific demonstration) to discover covert channels.

AVA_CCA.2-11 The evaluator ***shall examine*** the analysis documentation to determine that the method used to identify covert channels is shown to be repeatable.

24 A repeatable method is shown to yield consistent results given the same inputs.

1.4.2 AVA_CCA.2.2E

AVA_CCA.2.2E The evaluator shall confirm that the results of the covert channel analysis show that the TOE meets its functional requirements.

AVA_CCA.2-12 The evaluator ***shall examine*** the identified covert channels to determine that the TOE security policy is upheld.

25 For a covert channel to be harmful, the sender must be forbidden to communicate with the receiver under the TOE's security policy (as expressed by the TOE's security functional requirements and the Security Policy Model), and there must be an effective procedure for exploiting a security flaw to form a channel for transmitting a useful quantity of information from sender to receiver in a timely fashion.

1.4.3 AVA_CCA.2.3.E

AVA_CCA.2.3E The evaluator shall selectively validate the covert channel analysis through testing.

AVA_CCA.2-13 The evaluator ***shall devise*** a test subset

26 The evaluator selects a test subset and testing strategy that is appropriate for the TOE. Where the TOE includes only a small number of covert channels, it may be practical to rigorously test all of the channels. For TOEs with a large number of identified covert channels this will not be cost-effective, and sampling is required. For guidance on sampling see CEM B.2.

27 Covert channel testing demonstrates that covert channel handling methods chosen by system designers work as intended. These methods include covert channel elimination, bandwidth limitation, and (ability to) audit.

28 Testing is also used to confirm that potential covert channels discovered in the system are in fact real channels. Furthermore, testing is useful when the handling method for covert channels uses variable bandwidth-reduction parameters (e.g., delays) that are settable by system administrators (e.g., by auditors).

29 Bandwidth estimation methods necessary for the handling of covert channels may be based on engineering estimation rather than on actual measurements. Bandwidth estimations provide upper bounds for covert channels before employing any handling methods. In contrast, covert channel testing always requires doing actual measurements to determine the covert channel bandwidths after implementing the chosen handling method in a system.

AVA_CCA.2-14 The evaluator ***shall produce*** test documentation for the test subset that is sufficiently detailed to enable the tests to be reproducible.

30 With an understanding of the expected behaviour of the covert channel, the evaluator has to determine the most feasible way to test the channel. Specifically the evaluator considers:

a) the approach that will be used;

b) the interface(s) that will be used to test the channel;

c) the initial conditions that will need to exist for the test (i.e. any particular objects or subjects that will need to exist and security attributes they will need to have);

d) special test equipment that will be required to either stimulate the interfaces (e.g. packet generators) or make observations (e.g. network analysers).

31 The evaluator's test documentation should specify the derivation of each test, tracing it back to the portions of the analysis documentation.

AVA_CCA.2-15 The evaluator ***shall conduct*** testing.

32 The test documentation is used as a basis for testing but this does not preclude the evaluator from performing additional ad hoc tests. The evaluator may devise new tests based on behaviour of the TOE discovered during testing. These new tests are recorded in the test documentation.

AVA_CCA.2-16 The evaluator ***shall record*** the following information about the tests that compose the test subset:

a) identification of the covert channel to be tested;

b) instructions to connect and setup all required test equipment as required to conduct the test;

c) instructions to establish all prerequisite test conditions;

d) instructions to stimulate the requisite interfaces;

e) instructions for observing the behaviour of the TOE;

f) descriptions of all expected results and the necessary analysis to be performed on the observed behaviour for comparison against expected results;

g) instructions to conclude the test and establish the necessary post-test state for the TOE;

h) actual test results.

33 The level of detail should be such that another evaluator could repeat the tests and obtain an equivalent result. While some specific details of the test results may be different (e.g. time and date fields in an audit record) the overall result should be identical.

AVA_CCA.2-17 The evaluator ***shall check*** that all actual test results are consistent with the expected test results.

34 Any differences in the actual and expected test results may indicate that the developer covert channel analysis is incorrect. Unexpected actual results may require corrective corrections to the covert channel analysis and perhaps require rerunning of relevant tests and modifying the test sample size and composition. This determination is left to the evaluator, as is its justification.