Downloaded from http://www.everyspec.com

DATA ITEM DESCRIPTION

Title: Covert Channel Analysis Report

Number: DI-MISC-81345A
AMSC Number: 9029
DTIC Applicable: No
Office of Primary Responsibility: NS/I735
Applicable Forms: N/A

Approval Date: 28 Nov 2007
Limitation: N/A
GIDEP Applicable: No

Use/Relationship:

The Covert Channel Analysis Report documents the results of a covert channel analysis performed on an Information Assurance (IA) product or system.

This Data Item Description (DID) contains the format and content preparation instructions for the data product generated by the specific and discrete task requirements as delineated in the contract.

This DID is applicable to any IA product or system defining a Type 1 security policy with information flow requirements.

This DID supersedes DI-MISC-81345.

Requirements:

1. Reference documents. None.

2. Format:

2.1 Document the Covert Channel Analysis as follows:

a. Cover Sheet. Shall contain Title, Contract Number, Procuring Activity, Contractor Identification, Acquisition Program Name, disclaimers (as provided by the procuring activity contracting officer), date, version number, security classification and any other appropriate descriptive data.

b. Errata Sheet. Shall contain delimiting cumulative page changes from previous versions.

c. Table of Contents. Shall contain paragraph numbers, paragraph names, and page numbers.

d. List of illustrations, diagrams, charts and figures.

e. Glossary of abbreviations, acronyms, terms, symbols, and notations used, and

Downloaded from http://www.everyspec.com

their definitions.

f. Executive Summary, not to exceed two pages, that briefly describes the Covert Channel Analysis Report.

g. Introductions.

h. Body of the Report

i. Attachments.

j. Subjective index

k. Appendixes.

l. Bibliography. List of reference sources and applicable documents.

2.2 Specific Format Instructions.

a. Abbreviations and acronyms shall be defined when first used in the text and shall be placed in the glossary.

b. Pages shall be numbered separately and consecutively using Arabic numerals. Blank pages shall be numbered.

c. Paragraphs shall have a short descriptive title and shall be numbered consecutively using Arabic numerals. Numbering schemes beyond the fourth level (e.g., 4.1.2.5.8) are not permitted.

d. Chapters shall begin on an odd-numbered (right hand) page.

e. Column headings shall be repeated on subsequent pages if tabular material exceeds one page.

3. Content: The Covert Channel Analysis Report shall contain the following items:

a. A description of the covert channel protection policy that mitigates violations to the information flow requirements. The policy shall document how the assurance required for the system is commensurate with the sensitivity of the information protected and risks associated with the technology and operating environment.

b. The covert channel protection policy shall specify the level of covert channel analysis (CCA), i.e., informal, systematic/formal, or exhaustive, required for the target system.

Downloaded from http://www.everyspec.com

c. For a systematic CCA, the analysis shall describe how it is structured and repeatable.

d. For an exhaustive CCA the analysis shall describe how it is structured, repeatable, and exercises all possible methods for determining the existence of covert channels.

e. The covert channel protection policy shall specify whether covert channels are to be documented, limited (in terms of capacity), monitored, or eliminated. For a particular system, multiple mitigations may be specified, and the distinction shall be based on the characteristics of an individual channel.

f. The CCA shall document the analysis of each information flow policy specified in the system security policy in terms of a potential covert channel.

g. The CCA shall document the analysis of both the design and implementation of the target system for potential covert channels. Low-level implementation details, including external interface definitions and source code or hardware logic specification shall be used as inputs to the analysis.

h. The CCA shall document the analysis all bypass policies for potential creation of covert channels.

i. The CCA shall identify each covert channel and describe a worst-case exploitation scenario for the channel.

j. The CCA shall identify the characteristics of each channel, including but not limited to:
- categorization (storage or timing)
- capacity estimate (including the method used for estimation)
- direction (ingress, egress, bidirectional)
- encoding (direct or indirect)
- reliability (noisy or noiseless)

k. The CCA shall describe all assumptions made during the analysis and provide evidence that the level of analysis and mitigation complies with the specified policy. An example of such an assumption would be the relative physical or logical location of the processes participating in the covert communication. For example, for an inline network encryptor, the processes could be hosts residing on the plaintext and ciphertext networks. Alternatively, a covert channel could require malicious code to be executing in the network processors themselves.

4. End of DI-MISC-81345A