NPS-CAG-14-008

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

Trusted Computing Exemplar:
Low-level Design Document Standards
by

Paul C. Clark, Cynthia E. Irvine, and Thuy D. Nguyen

12 December 2014

Prepared for: United States Navy, OPNAV N2/N6

THIS PAGE INTENTIONALLY LEFT BLANK

NAVAL POSTGRADUATE SCHOOL
Monterey, California 93943-5000

Ronald A. Route
President

Douglas A. Hensler
Provost

The report entitled "Trusted Computing Exemplar: Low-level Design Document Standards" was prepared for United States Navy, OPNAV N2/N6 and funded in part by United States Navy, OPNAV N2/N6.

Further distribution of all or part of this report is authorized.

This report was prepared by:

Paul C. Clark
Research Associate

Cynthia E. Irvine
Distinguished Professor

Thuy D. Nguyen
Research Associate

Reviewed by:

Cynthia E. Irvine, Chair
Cyber Academic Group

Released by:

Jeffrey D. Paduan
Dean of Research

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From-To)*
12-12-2014	Technical Report	Nov 2013 to Nov 2014

4. TITLE AND SUBTITLE
Trusted Computing Exemplar: Low-level Design Document Standards Standards

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Paul C. Clark, Cynthia E. Irvine, and Thuy D. Nguyen

5d. PROJECT NUMBER
W4C05

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER
NPS-CAG-14-008

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Rhonda Onianwa
OPNAV, N2N6 F13
rhonda.onianwa@navy.mil

LT David Rivera
OPNAV, N2/N6F1
david.j.rivera4@navy.mil

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for pubic release; distribution is unlimited

13. SUPPLEMENTARY NOTES
The view expressed in this report are those of the authors and do not reflect the official policy or position of the Department of Defense of the U.S. Government.

14. ABSTRACT

This document describes the Life Cycle Management Plan for the development of a high assurance secure product. A high assurance product is one for which its users have a high level of confidence that its security policies will be enforced continuously and correctly. Such products are constructed so that they can be analyzed for these characteristics. Lifecycle activities ensure that the product reflects the intent to ensure that the product is trustworthy and that vigorous efforts have been made to ensure the absence of unspecified functionality, whether accidental or intentional.

This document provides the standard format for writing low-level design documents.

Low-level design documents provide a detailed description of one or more modules. The level of detail should be sufficient such that two independent implementations will produce functionally equivalent modules.

15. SUBJECT TERMS
Machinery control systems, MCS, life cycle security, high assurance, system security, trustworthy systems

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			Cynthia E. Irvine
Unclassified	Unclassified	Unclassified	UU	15	**19b. TELEPHONE NUMBER** *(include area code)* (831) 656 2461

Standard Form 298 (Rev. 8-98)

Prescribed by ANSI Std. Z39.18

THIS PAGE INTENTIONALLY LEFT BLANK

CYBER ACADEMIC GROUP
NAVAL POSTGRADUATE SCHOOL

NPS-CAG-14-008

Trusted Computing Exemplar: Low-level Design Document Standards

Paul C. Clark
Cynthia E. Irvine
Thuy D. Nguyen

December 2014

ATTRIBUTION REQUEST

December 2014

The Cyber Academic Group (CAG) and the Center for Information Systems Security Studies and Research (CISR) at the Naval Postgraduate School (NPS) wish to facilitate and encourage the development of highly robust security systems.

To further this goal, the NPS CAG and NPS CISR ask that any derivative products, code, writings, and/or other derivative materials, include an attribution for NPS CAG and NPS CISR. This is to ensure that the public has a full opportunity to direct questions about the nature and functioning of the source materials to the original creators.

ACKNOWLEDGEMENT

The authors gratefully acknowledge the following organizations for providing support toward the development of this work: OPNAV N2/N6 F1.

The material presented here builds upon work supported in previous years by the Office of Naval Research.

A portion of the material presented here is based upon work supported by the National Science Foundation under Grant No. CNS-0430566 and CNS-0430598. This document does not necessarily reflect the views of the National Science Foundation.

Table of Contents

[THIS PAGE IS INTENTIONALLY BLANK]

1 Introduction

This document has been written in support of a research project to publicly demonstrate and document how a high assurance product can be developed and distributed. A high assurance product is one for which its users have a high level of confidence that its security policies will be enforced continuously and correctly. Such products are constructed so that they can be analyzed for these characteristics. Lifecycle activities ensure that the product reflects the intent to ensure that the product is trustworthy and that vigorous efforts have been made to ensure the absence of unspecified functionality, whether accidental or intentional.

This document provides the standard format for writing low-level design documents.

Low-level design documents provide a detailed description of one or more modules. The level of detail should be sufficient such that two independent implementations will produce functionally equivalent modules.

2 Document Structure

Low-level design documents shall be structured according to the following format. Data types shall be provided for all databases, database elements, constants, variables, inputs, outputs, functions, and error messages.

2.1 Introduction

2.1.1 Module Description

This section shall provide a brief description of the module(s) under design.

2.1.2 Abbreviations

This section shall provide a list of all abbreviations and acronyms used in the design.

2.2 Low-level Design Constraints

This section shall provide a list of requirements, with descriptions, related to the module(s) under design. This section may be further divided into subsections if necessary, desirable, or appropriate. Requirements the module(s) must meet which are listed in other documents shall not be repeated here.

2.3 Constants

This section shall list all constants, with data types, used in the design. This section may be further divided into subsections if necessary, desirable, or appropriate. Module-specific constants shall not be listed here, but shall be listed in the appropriate module subsection.

2.4 Database

This section shall contain a subsection for each database used in the design. Each subsection shall describe the database, list the organization of the database (the fields it contains, including data types), list any constraints on the database (e.g. it is not modifiable during run-time), and specify the module that manages the database.

2.5 Layering

This section shall contain a subsection for each layer used in the design. Each subsection shall list the modules contained within the layer.

2.6 Modules

This section shall contain a subsection for each module used in the design. Each subsection shall describe the module in terms of the interfaces it provides, including function name and a brief description of the purpose of the function. Each subsection shall also describe any module specific constants. Each module shall be identified as either a module that enforces a security policy, or a module that supports the enforcement of a security policy, or a module that is non-security-relevant. For each module, the lower-layer modules upon which it depends shall be listed in each subsection. The detailed design of the module is not included in this section.

2.7 Detailed Design

This section shall contain a subsection for each module used in the design. Each subsection shall describe the detailed implementation of the module. The format of each subsection shall be as follows:

2.7.1 Module name

Include a brief description of the module.

2.7.1.1 Internal Constants

Include a list of internal constants, with data types, used by the module.

2.7.1.2 Module data

Include a list of internal data, with data types, used by the module. This includes the database that the module manages.

2.7.1.3 Module functions

This section is repeated for each module function. Module interface functions shall be listed first, followed by module internal functions, if necessary. Each function section shall consist of a brief description of the function, a C language prototype of the function (including data types for inputs, outputs, and the function return value, if any), and the following subsections:

2.7.1.3.1 Inputs

This section shall contain a list of each input to the function. The list shall contain a description of the input, and any restrictions on the input, if applicable.

2.7.1.3.2 Processing

This section shall describe the processing of the function. The processing shall be listed in sequential order. Indentation shall be used to differentiate conditional processing, or repeated (looping) processing. The descriptions shall use natural language with reference to module data and constants as appropriate. The use of other modules (function calls into other modules) shall include the name of the function called, the parameters passed to the function, the outputs from the function, and the name of the module being called.

2.7.1.3.3 Outputs

This section shall contain a list of each output from the function, including a function return value, if applicable. The list shall contain a description of each output. If a function return value is included, then the possible values, including exceptions, shall be listed and described.

2.7.1.3.4 Effects

This section shall describe the effects of invoking the function.

2.7.1.3.5 Error messages

This section shall describe any error messages generated by the function.

References

The following were referenced directly in this document.

[1] *Common Criteria for Information Technology Security Evaluation*, version 2.2, 2004.

[THIS PAGE IS INTENTIONALLY BLANK]

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center 2
   Ft. Belvoir, Virginia

2. Dudley Knox Library, Code 013 2
   Naval Postgraduate School
   Monterey, California 93943

3. Research Sponsored Programs Office, Code 41 1
   Naval Postgraduate School
   Monterey, California 93943

4. Paul C. Clark 1
   Naval Postgraduate School
   Monterey, California 93943

5. Dr. Cynthia E. Irvine 1
   Naval Postgraduate School
   Monterey, California 93943

6. Thuy D. Nguyen 1
   Naval Postgraduate School
   Monterey, California 93943