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

Approved for public release; distribution is unlimited

Prepared for: United States Navy, OPNAV N2/N6
THIS PAGE INTENTIONALLY LEFT BLANK

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

This report was prepared by:

________________________________________  ________________________________________
Paul C. Clark                                      Cynthia E. Irvine
Research Associate                                Distinguished Professor

________________________________________
Thuy D. Nguyen
Research Associate

Reviewed by:                                      Released by:

________________________________________  ________________________________________
Cynthia E. Irvine, Chair                          Jeffrey D. Paduan
Cyber Academic Group                             Dean of Research
# Trusted Computing Exemplar: Low-level Design Document Standards

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.

## Subject Terms
Machinery control systems, MCS, life cycle security, high assurance, system security, trustworthy systems

## Security Classification of:

| a. REPORT | Unclassified |
| b. ABSTRACT | Unclassified |
| c. THIS PAGE | Unclassified |

## Limitation of Abstract

| 17. LIMITATION OF ABSTRACT | UU |

## Number of Pages

| 18. NUMBER OF PAGES | 15 |

## Name of Responsible Person

| 19a. NAME OF RESPONSIBLE PERSON | Cynthia E. Irvine |

## Telephone Number

| 19b. TELEPHONE NUMBER (include area code) | (831) 656 2461 |

Approved for public release; distribution is unlimited.

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.

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.
Trusted Computing Exemplar: Low-level Design Document Standards

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

December 2014
ATTENTION 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

1 Introduction ......................................................................................................................... 1

2 Document Structure ........................................................................................................... 1
   2.1 Introduction .................................................................................................................... 1
   2.2 Low-level Design Constraints ....................................................................................... 1
   2.3 Constants ....................................................................................................................... 1
   2.4 Database ....................................................................................................................... 2
   2.5 Layering ......................................................................................................................... 2
   2.6 Modules ......................................................................................................................... 2
   2.7 Detailed Design ............................................................................................................ 2

References ............................................................................................................................... 3
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.

2004.
INITIAL DISTRIBUTION LIST

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

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

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

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

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

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