NPS-CAG-14-003

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

Trusted Computing Exemplar:
Confuguration Management Plan

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

NAVAL POSTGRADUATE SCHOOL
Monterey, California 93943-5000

Ronald A. Route President	Douglas A. Hensler Provost

The report entitled "Trusted Computing Exemplar: Configuration Management Plan" 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:	**Released by:**
Cynthia E. Irvine, Chair Cyber Academic Group	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)*** 12-12-2014	**2. REPORT TYPE** Technical Report	**3. DATES COVERED** ***(From-To)*** Nov 2013 to Nov 2014

4. TITLE AND SUBTITLE
Trusted Computing Exemplar: Configuration Management Plan

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-14-003

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.

The purpose of this document is, first, to describe the high-level procedures and policy for Configuration Management (CM), and, second to create a CM plan that aims to ensure the integrity of the configuration items, track changes to the configuration items, and ensure that only authorized changes are made to the configurations items.

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 Unclassified	**b. ABSTRACT** Unclassified	**c. THIS PAGE** Unclassified	UU	17	Cynthia E. Irvine
					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-14-003

Trusted Computing Exemplar: Configuration Management Plan

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

Table of Tables

1 Purpose

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.

The Common Criteria (CC) [1] was used as a guide to determine the necessary steps that would lead to a high assurance product.

The purpose of this document is described below:

1. This document describes the high-level procedures and policy for Configuration Management (CM).
2. The objectives of this CM plan include: ensuring the integrity of the configuration items, tracking changes to the configuration items, and ensuring only authorized changes are made to the configurations items.

2 Scope

1. The items to be managed under this plan include any documents, source code, specifications, and other items written, used or developed, including bug reports, security flaws, and development tools, as part of the product development process. These items shall be listed in the document entitled 'Configuration Item List', which itself shall be managed according to this plan.
2. This plan applies to engineering documentation, manuals, reports, hardware, firmware, and software related to the product being developed.

3 Functions and Responsibilities

1. Configuration Manager - The Configuration Manager is responsible for ensuring that procedures and policies of this CM plan are followed throughout the development process. The Configuration Manager is also responsible for ensuring the integrity of items placed under CM, and for ensuring that configuration items are not accepted into CM by the person who developed the configuration item. The Configuration Manager shall place into CM only those items approved by the Change Control Board (CCB) and shall only accept those items from the CCB, not directly from a developer. The Configuration Manager is responsible for recording and archiving the minutes of the CCB meetings.
2. Project Manager - The Project Manager is responsible for the overall direction and management of the project. Additionally, the Project Manager is responsible for conducting audits of the CM system, and procedures, as defined in 'Audits and Reviews' (see Section 7).

3. Configuration Item leader - The Configuration Item leader is responsible for managing the development of a particular Configuration Item (CI). In the case of CM issues, the CI leader is responsible for reviewing, and approving/denying, all change requests for the particular CI before submitting the change requests to the CCB.
4. Security Analyst - The Security Analyst is responsible for ensuring that all security relevant aspects of a change request are considered. The Security Analyst takes a big picture view, keeping in mind the entire project, not just a single CI.
5. CCB Chair - The CCB Chair is appointed by the Configuration Manager, and is responsible for running the CCB meetings and resolving any conflicts that might arise between the different participants.
6. Change Control Board - The Change Control Board (CCB) is responsible for ensuring that the change control procedures outlined in this CM plan are followed. The CCB shall be made up of the Project Manager, the Configuration Manager, the Security Analyst, the Configuration Item leader(s) and members of the technical development staff. The CCB has the authority for approving change requests. Unanimous approval by all CCB members is required for all change requests.
7. Technical Development Staff - Each member of the development staff is responsible for following the procedures and policies outlined in this plan. This includes reviewing technical content pertaining to change requests.

4 Configuration Item Identification

Items to be managed by this plan shall have a unique identifier. Since this plan is intended to apply to multiple projects, the identifier shall consist of two parts: the first part identifying the project the item belongs to, and the second part shall be an identifier of the item within the project. Each project shall document how Configuration Items are uniquely identified.

5 Change Control

1. All changes to configuration items, including the initial version of an item, shall be reviewed and approved according to the following procedure.
    a. A change request shall be completed for each change, as described in the *Configuration Management Procedures*. [2]
    b. Each change request shall be tracked by the CM system. When a change is submitted to the CCB, it shall be assigned a 'change request number' and status. The status for a change request shall be one of the following:

    Pending
    The change request has been submitted to the CCB
    Approved
    The change request has been approved by the CCB
    Completed
    The change request is complete, and all items have been checked into CM. The change request itself is placed into CM.
    Resubmit

The change request has been denied by the CCB; a resubmittal is possible.

Denied

The change request has been denied by the CCB, no further action shall be taken on the request. The change request itself is placed into CM.

Table 1 Change Request States

State	Action	Signature	New State
-	Submit Change Request to CCB	Originator and CI leader	Pending
Pending	Deny Change Request	CCB chair	Denied
Pending	Approve Change Request	CCB chair and Project Manager	Approved
Pending	Ask for Resubmittal	none	Resubmit
Resubmit	Correct/Update items and Change Request	CI leader	Pending
Approved	Place items into CM	Configuration Manager	Completed

c. All pending configuration items to be changed shall be listed on the change request form. The change request shall document the reason for the change, as well as actual changes to the configuration item.

d. If new items are to be added, unique identifiers shall be assigned to them, and they shall be added to the 'Configuration Item List' for the project.

e. Items to be changed shall be reviewed by the CI leader to verify that the change is consistent across all relevant, or related, parts of the project. Changes to externally visible interfaces, whether at the project level, or for an internal component, shall include changes to the appropriate specifications, and user manuals.

f. The CCB shall review, and approve/deny/ask for resubmittal, all change requests. All changes shall be reviewed and accepted according to the Acceptance Plan (see below).

g. With the exception of the 'Resubmit' state, all changes in the state of a change request shall require the signature of the person(s) identified in Table 1.

h. Change requests eligible for resubmittal shall be sent back to the CI leader with directions for corrective actions before the change request can be resubmitted to the CCB.

i. For each approved change request, the Configuration Manager shall ensure that the reviewed items are placed into CM. The Configuration

Manager shall also set the status of the change request to Completed, and place the change request into CM.

j. For each denied change request, the Configuration Manager shall set the status of the change request to Denied, and place the change request into CM.

6 Status Accounting

1. The CM system shall track the status of each configuration item, as well as the status of change requests.
2. For each configuration item, the CM system shall be able to report:
   a. The current version.
   b. For each change to a configuration item: the date of the change; the person responsible for the change; the change request number.
   c. Differences between any two versions of a CI.
3. For each change request that has been submitted to the CCB, the CM system shall be able to report:
   a. The status of the change request.
4. For each Completed change request, the CM system shall be able to report:
   a. The date of the change
   b. The person responsible for the change
   c. A complete list of all items changed
5. For each project, the CM system shall be able to report:
   a. A complete list of all configuration items.
   b. All change requests for items within the project.

7 Audits and Reviews

1. An audit of the CM procedures shall consist of periodic reviews of Completed change requests. The reviews shall determine that each change described in the change request is reflected in the CM system. Additionally, the change request shall be reviewed for completeness (e.g., signatures).
2. As a cross check, periodic reviews of selected CI's shall be performed to ensure that all changes are documented in completed change requests.
3. The Project Manager shall be responsible for determining how often the CM audit is performed, as well as selecting the non-CM staff to do the audit.

8 CM System Tools and Usage

1. To support the automated generation of the product, the CM system shall be able to provide a read-only master copy of all CIs that make up the product.
2. To ensure the integrity of the items in CM, the developer/modifier of a CI shall not be the person that accepts the CI into CM.
3. The CM tools and procedures are documented in the CM System Users Guide.

9 Protection of CM System

1. The computer system that hosts the CM system and configuration item storage shall be protected from modification by people and computers external to the

project. To do this the CM system shall be isolated from other computers and networks. All transfers of changed CIs to the CM system shall be done using removable media (e.g., CDs). All retrieval of CIs from the CM system shall also be done using removable media.

2. As a further precaution, only staff authorized to accept CI changes shall be given access to the CM system.
3. The Configuration Manager shall be responsible for ensuring all CM related items in paper form (e.g. Change Requests) are protected.

References

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

[2] P. C. Clark, C. E. Irvine, T. Levin, T. D. Nguyen, and D. Warren, “Trusted Computing Exemplar: Configuration management procedures,” Naval Postgraduate School, Monterey, CA, Tech. Rep. NPS-CAG-14-004, Dec. 2014.

Appendix A – Naming Convention for Files and Directories

Files destined to be baselined into the CM file tracking system, and the directory structure for those files, shall adhere to the following restrictions:

- Only the following characters can be used for names: A-Z, a-z, 0-9, '.' [period], '_' [underscore], '-', hyphen.
- Upper-case is allowed, as long as there is uniqueness of all names maintained within the same directory when names are normalized to lower-case.
- Names shall not begin or end with a period.
- Only one period shall be used per name.
- The following names shall not be used: com[1-9], lpt[1-9], con, nul, prn.

These restrictions will eliminate cross-platform file name incompatibilities, problems with file transfer, as well as problems dealing with other characters when writing scripts to process files.

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