NPS-CAG-14-006

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

Trusted Computing Exemplar:
Physical Security Plan

by

Paul C. Clark, Phil Hopfner, 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: Physical Security 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

Phil Hopfner
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	Nov 2013 to Nov 2014

4. TITLE AND SUBTITLE
Trusted Computing Exemplar: Physical Security Plan

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Paul C. Clark, Phil Hopfner, 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-14-006

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 plan is to provide the policy necessary to ensure the physical protection of the product during its entire life cycle. Product integrity is the primary concern, though confidentiality is not disregarded.

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	17	**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-14-006

Trusted Computing Exemplar: Physical Security Plan

Paul C. Clark
Phil Hopfner
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.

The purpose of this plan is to provide the policy necessary to ensure the physical protection of the product during its entire life cycle. Product integrity is the primary concern, though confidentiality is not disregarded.

2 [Organization Name Here]

This section describes the physical security of the organization that is developing the product.

3 Policy

This section provides the policy statements with respect to physical security of high assurance product development.

1. The physical security requirements of sponsoring organizations or customers shall be complied with.

2. The development servers shall be physically protected.

   The servers that store electronic files under development for a project shall be physically and logically accessible to authorized personnel only. (See the *Personnel Security Plan* [1] for information about authorized users). The server shall reside in the physically protected office of an authorized developer, or a locked room with controlled access, or in a locked rack in an area where unauthorized users have access.

3. The Configuration Management (CM) network shall be physically protected and isolated.

   The network of systems dedicated to CM shall not be networked to non-CM systems in any way. They shall only be physically accessible to project personnel, and they shall only have user accounts for the CM manager and CM staff. Developers shall not have accounts on CM systems.

4. The development network shall be physically or logically separated from any other network.

The network that supports the development of a high assurance project shall not have connectivity to other networks.

5. Keys and combinations shall be controlled.

   When keys are used to control physical access, key control policies will be established and followed. When combinations are used to control physical access, the combinations will be changed no less than quarterly, or whenever someone who knows the combination separates from the project, whichever comes first. When combinations are used to control physical access to cabinets, the combinations will be changed whenever someone who knows the combination separates from the project.

6. Project data under development should be stored on the development servers.

   If a client system has only limited physical protection, then project data shall not be allowed on the client system. Such clients shall access project data remotely in such a way that the data remains on the server and is not copied to the client. If a client system has physical protection such that only authorized personnel have access to it, then project data can be temporarily copied to the client system, but changes shall be copied back to the server so they can be properly backed up.

7. A backup plan shall be established and followed for both the development servers and the CM server. (See Appendix A for the backup plan for the development server).

   The plan must prepare for the following kinds of disasters:
   a. Human error
   b. Disk error
   c. Theft of servers
   d. Physical disasters

8. Backup media shall be physically protected.

   The backup media shall be protected to at least the same degree as the systems they refer to.

9. Visitors

   Visitors are allowed in the physical presence of the project servers when escorted by authorized personnel.

10. Audits

Unscheduled checks of the physical security measures will be made. Examples of auditable items:

a. Verification that doors and cabinets are locked.
b. Verification that backups are being performed according to plan.
c. Verification that all backup media is accounted for.
d. Verification that systems on the development network cannot access outside networks, and that outside networks cannot access the development network.

All audits, and their results, are to be documented. Violations of policy shall be brought to the attention of the CCB to determine the appropriate course of action.

11. The configuration of the following systems are controlled by the CCB:
    - Development clients
    - Development servers
    - Configuration management clients
    - Configuration management server
    - Formal verification clients
    - Formal verification server

    Any installation or removal of software, including patches, must be approved ahead of time. Any change in the configuration of the systems must be approved ahead of time. This does not include the adding and removing of accounts, which is covered in the *Personnel Security Plan* [1].

    It is recognized that issues arise that require a system administrator to debug project hardware and software to determine the cause of a problem. Such debugging may require the ad-hoc modification of settings, un-installation of CCB-approved software, etc. In such cases, the system administrator is granted approval to apply reasonable practices to identify the problem. However, careful notes of all changes shall be taken. If the changes that fix the problem would normally require CCB approval, then the Project Manager may approve them in order to get the system back online, but the change must be submitted to the CCB for ratification.

4 Responsibilities

This section assigns responsibility for meeting the requirements of this document.

1. Organizational security personnel.

   This paragraph shall describe the expected security practices and procedures of the security personnel within the associated organization.

2. Change Control Board (CCB)

   The CCB oversees the physical security of the development and CM systems, including the oversight of physical security audits.

3. System Administrators

   The system administrators are responsible for performing the backups as specified by the development server backup plan, and to properly store the backup media.

   The system administrators are responsible for properly configuring the systems on the development network to prevent access to other networks.

4. Lab Manager

   An assigned manager or authorized user shall be responsible for changing the combinations and managing the physical keys as required.

5. Authorized Personnel

   All personnel associated with the a high assurance project have a responsibility to be familiar with the physical security policies defined herein, to comply with them, and to report any violations in a timely fashion.

References

P.C. Clark, C. E. Irvine, T. Levin, and T. D. Nguyen, “Trusted Computing Exemplar: Personnel security plan,” Naval Postgraduate School, Monterey, CA, Tech. Rep. NPS-CAG-14-005, Dec. 2014.

Appendix A – Development Server Backup Plan

This appendix lays out the minimal requirements for the preservation of project data on the development server.

1. Backup Frequency

   Once per week: Full manual backup of project data to removable media that is stored away from the servers.

   Every workday: Full automated backup of project data to an external device that is not removed from the servers.

   Other: An image backup of the servers shall be made after initial setup and after configuration changes are made.

2. Verification

   If the backup software provides the functionality, backups shall be verified. Verification shall be performed before a log entry is made (see below).

3. Rotation of Media

   The weekly backup shall be kept for four weeks before it is put back into the rotation.

   The last weekly backup of the month shall be removed from the rotation for twelve months before it is put back into the rotation.

   The last weekly backup of the year shall be archived for permanent storage.

4. Off-Site Storage

   The last weekly backup of the month, and the last weekly backup of the year shall be stored off-site.

5. Reliability

   CDs shall not be used for backup media, due to reliability problems.

6. Documentation Requirements

   Procedures: The person performing the backups shall follow written established procedures.

   Media: The backup media shall be marked with the date of the backup, the name of the system it was used on, and the type of backup (weekly, monthly, yearly).

Log: A notation shall be made in a log indicating that the backup has been performed, including the date and time, and whether the backup has been verified. Any errors or abnormal performance shall also be noted in the log.

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