Raytheon Oakley Systems, Inc.
FIPS Linux Cryptographic Module

(Software Version: 1.0)

FIPS 140-2
Non-Proprietary Security Policy

Level 1 Validation

Document Version 0.3

Prepared for:

Raytheon
Oakley Systems

Raytheon Oakley Systems, Inc.
2755 E. Cottonwood Parkway, Suite 600
Salt Lake City, UT 84121
Phone: (801) 733-1100
Fax: (805) 583-0124
http://www.oakleynetworks.com

Prepared by:

Corsec

Corsec Security, Inc.
10340 Democracy Lane, Suite 201
Fairfax, VA 22030
Phone: (703) 267-6050
Fax: (703) 267-6810
http://www.corsec.com

Revision History

Version	Modification Date	Modified By	Description of Changes
0.1	2009-01-28	Darryl H. Johnson	Initial draft.
0.2	2009-03-11	Darryl H. Johnson	Addressed lab comments.
0.3	2009-04-13	Darryl H. Johnson	Addressed lab comments.

Table of Contents

Table of Figures

List of Tables

1 Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the Raytheon Oakley Systems FIPS Linux Cryptographic Module from Raytheon Oakley Systems, Inc.. This Security Policy describes how the Raytheon Oakley Systems FIPS Linux Cryptographic Module meets the National Institute of Standards and Technology (NIST) and the Canadian Security Establishment Canada (CSEC) requirements for cryptographic modules as specified in Federal Information Processing Standards Publication (FIPS PUB) 140-2. This document also describes how to run the module in its Approved FIPS 140-2 mode of operation. This policy was prepared as part of the Level 1 FIPS 140-2 validation of the module.

The Raytheon Oakley Systems FIPS Linux Cryptographic Module is referred to in this document as the cryptographic module, the software module, or the module.

1.2 References

This document deals only with operations and capabilities of the module in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the module from the following sources:

- The Raytheon Oakley website (http://www.oakleynetworks.com/) contains information on the full line of products from Raytheon Oakley.
- The NIST Cryptographic Module Validation Program (CMVP) website (http://csrc.nist.gov/groups/STM/index.html) contains information about the FIPS 140-2 standard and validation program. It also lists contact information for answers to technical or sales-related questions for the module.

1.3 Document Organization

The Security Policy document is one document in a FIPS 140-2 Submission Package. In addition to this document, the Submission Package contains:

- Vendor Evidence document
- Finite State Machine document
- Executive Summary document
- Other supporting documentation as additional references

This Security Policy and the other validation submission documentation were produced by Corsec Security, Inc. under contract to Raytheon Oakley. With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 validation documentation is proprietary to Raytheon Oakley and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Raytheon Oakley.

2 Raytheon Oakley Systems FIPS Linux Cryptographic Module

2.1 Overview

The Raytheon Oakley Systems FIPS Linux Cryptographic Module is a software module that provides the cryptographic functionality for the Raytheon Oakley Systems InnerView insider threat product.

InnerView is an information assurance technology solution that helps government agencies detect, prevent, and resolve insider policy violations. The InnerView product employs agent-based monitoring of targeted user activities across an organization's desktops and network, including mobile and offline users, and allows selected views into the major user communications channels (such as encrypted web traffic, email, and email attachments). InnerView provides DVR[1]-like incident replay, which allows an organization to take targeted action on acceptable use violations and provides powerful forensic support for investigations into more serious fraud, theft, and other malicious threats.

In FIPS 140-2 terminology, the FIPS Linux Cryptographic Module is a multi-chip standalone software module that meets the Level 1 FIPS 140-2 requirements. The module was tested and found to be compliant with FIPS 140-2 requirements on a general-purpose computer (GPC) with an Intel Xeon x86 processor running Red Hat Enterprise Linux (RHEL) 4 operating system (OS).

The Raytheon Oakley Systems FIPS Linux Cryptographic Module includes implementations of the following FIPS-Approved algorithms:

- Advanced Encryption Standard (AES)
- Secure Hash Algorithm (SHA-1)
- Keyed-Hash Message Authentication Code (HMAC) using SHA-1

The module always operates in a FIPS-Approved mode of operation.

The FIPS Linux Cryptographic Module is validated at the following FIPS 140-2 section Levels:

Table 1 – Security Level Per FIPS 140-2 Section

Section	Section Title	Level
1	Cryptographic Module Specification	1
2	Cryptographic Module Ports and Interfaces	1
3	Roles, Services, and Authentication	1
4	Finite State Model	1
5	Physical Security	N/A
6	Operational Environment	1
7	Cryptographic Key Management	1
8	EMI/EMC[2]	1

[1] DVR – digital video player

[2] EMI/EMC – Electromagnetic Interference / Electromagnetic Compatibility

Section	Section Title	Level
9	Self-tests	1
10	Design Assurance	1
11	Mitigation of Other Attacks	N/A

2.2 Cryptographic Boundary

2.2.1 Logical Cryptographic Boundary

Figure 1 below shows a logical block diagram of the module executing in memory and its interactions with surrounding components, as well as the logical cryptographic boundary of the module.

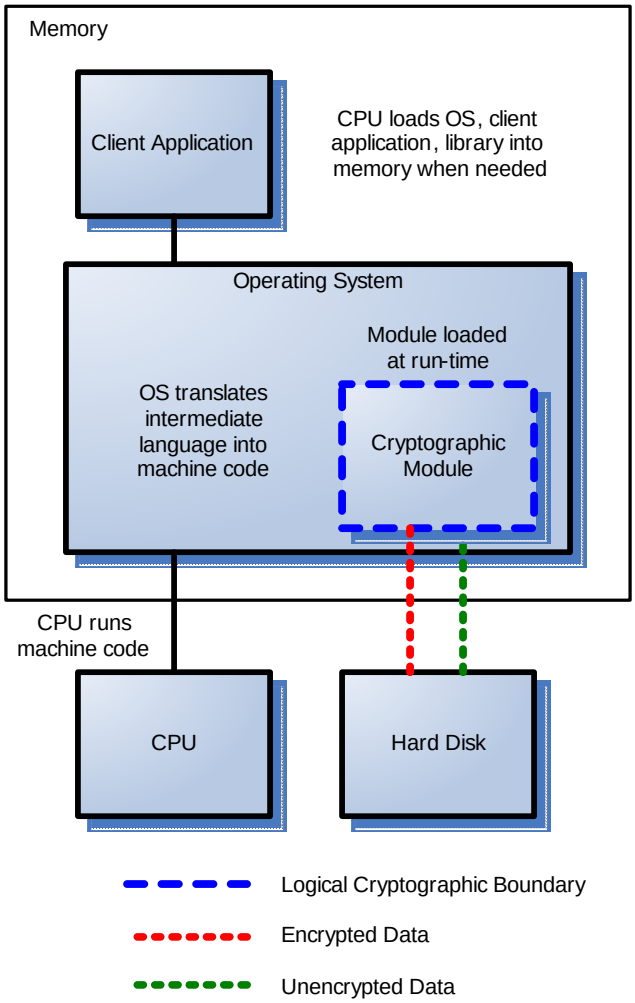

Figure 1 – Logical Block Diagram and Cryptographic Boundary[3]

[3] CPU – Central Processing Unit

2.2.2 Physical Cryptographic Boundary

As a software cryptographic module, there are no physical protection mechanisms implemented; the module must rely on the physical characteristics of the host machine. The physical cryptographic boundary of the FIPS Linux Cryptographic Module is defined by the hard metal enclosure around the computer on which it runs. The module supports the physical interfaces of a GPC. The physical interfaces include the mouse and keyboard ports, optical drives, floppy disk, serial ports, parallel ports, networks ports, monitor port, and power plug. See Figure 2 for a standard GPC block diagram.

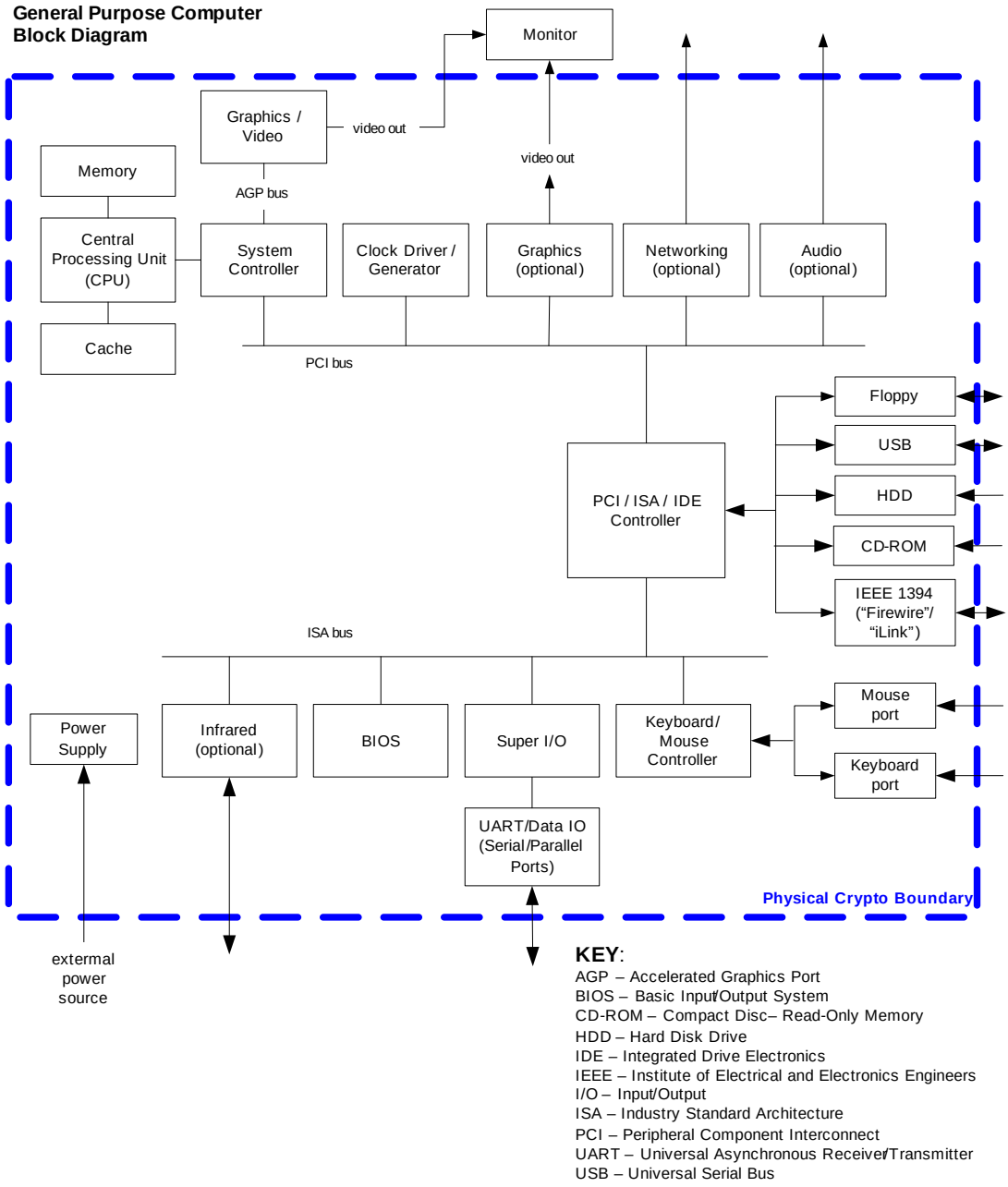

Figure 2 – Standard GPC Block Diagram

2.3 Module Interfaces

The module's logical interfaces exist in the software as an Application Programming Interface (API). Physically, ports and interfaces are considered to be those of the host server. Both the API and physical interfaces can be categorized into following logical interfaces defined by FIPS 140-2:

- Data Input Interface
- Data Out Interface
- Data Control Interface
- Status Output Interface
- Power Interface

A mapping of the FIPS 140-2 logical interfaces, the physical interfaces, and the module can be found in Table 2.

Table 2 – Logical, Physical, and Module Interface Mapping

FIPS 140-2 Logical Interface	Module Port/Interface	Module Mapping
Data Input	Keyboard, mouse, CD-ROM, floppy disk, and serial/USB/parallel/network ports	Function arguments that denote data to be used or processed by the module.
Data Output	Hard disk, floppy disk, monitor, and serial/USB/parallel/network ports	Function arguments that specify where the result of the function is stored.
Control Input	Keyboard, CD-ROM, floppy disk, mouse, and serial/USB/parallel/network port	Function calls utilized to initiate the module and the function calls used to control the operation of the module.
Status Output	Hard disk, floppy disk, monitor, and serial/USB/parallel/network ports	Return values for function calls
Power	Power Interface	N/A

2.4 Roles and Services

There are two roles in the module that operators may assume: a Crypto-Officer role and User role. The Crypto-Officer is responsible for managing the module and monitoring the module's status, while the User employs the functionality of the module. The available functions are utilized to provide or perform the cryptographic services.

The various services offered by the module are described below. The Critical Security Parameters (CSPs) used by each service are listed below.

2.4.1 Crypto-Officer Role

The Crypto-Officer is responsible for managing the module and monitoring the module's status. The Crypto-Officer can also execute the module's power-up self-tests on demand. Descriptions of the services available to the Crypto-Officer role are provided in Table 3.

Table 3 – Mapping of Crypto-Officer Role's Services to Inputs, Outputs, CSPs, and Type of Access

Service	Description	Input	Output	CSP and Type of Access
cbc_aes_init	Initializes the software module	Command	The module is loaded	None
cbc_aes_exit	Uninitializes the software module	Command	Module unloaded	None

Service	Description	Input	Output	CSP and Type of Access
proc_read_status	Runs self-tests on demand and monitor status	API call	Status output	None

2.4.2 User Role

The User role has the ability to perform encryption/decryption operations using the module. Descriptions of the services available to the User role are provided in Table 4.

Table 4 – Mapping of User Role's Services to Inputs, Outputs, CSPs, and Type of Access

Service	Description	Input	Output	CSP and Type of Access
aes_setkey	Sets key for AES cipher operation	API call	Status Output	Symmetric Key – Write
aes_encrypt	Performs AES encryption	API call with data	Status Output	Symmetric Key – Read
aes_decrypt	Performs AES decryption	API call with data	Status Output	Symmetric Key – Read

2.4.3 Authentication

The module does not support any authentication mechanism. Operators of the module implicitly assume a role based on the services of the module being used. Since all services offered by the module can only be used by either the Crypto-Officer or the User (never both), the roles are mutually exclusive. Thus, when the operator is using services listed in Table 3, he implicitly assumes the Crypto-Officer role. When the operator is using services listed in Table 4, he implicitly assumes the User role.

2.5 Physical Security

The cryptographic module is a software module and does not include physical security mechanisms. Thus, the FIPS 140-2 requirements for physical security are not applicable.

2.6 Operational Environment

The module is intended for use on a GPC with an Intel Xeon x86 processor running Red Hat Enterprise Linux 4. For FIPS 140-2 compliance, this is considered to be a single user operating system. As such, all keys, intermediate values, and other CSPs remain only in the process space of the operator using the module. The operating system uses its native memory management mechanisms to ensure that outside processes cannot access the process space used by the module.

2.7 Cryptographic Key Management

The module uses implementations of the following FIPS-Approved algorithms:

- Advanced Encryption Standard (AES) 128-, 192-, 256-bit keys in Cipher Block Chaining (CBC) mode – FIPS 197 (certificate #943)
- Secure Hash Algorithm (SHA-1) – FIPS 180-2 (certificate #919)
- Keyed-Hash MAC (HMAC) using SHA-1 (certificate #524)

The module supports the critical security parameters listed in Table 5 below.

Table 5 – List of Cryptographic Keys, Cryptographic Key Components, and CSPs

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
Symmetric Key	AES CBC key (128, 192, 256 bits)	Enters the module in plaintext	Never exits the module	Plaintext in volatile memory	By power cycle	Encrypts data

2.8 EMI / EMC

Although the module consists entirely of software, the FIPS 140-2 evaluated platform is a standard GPC, which has been tested for and meets applicable Federal Communications Commission (FCC) EMI and EMC requirements for business use as defined in Subpart B of FCC Part 15.

2.9 Self-Tests

The FIPS Linux Cryptographic Module automatically performs the following self-tests at power-up:

- Software integrity check using HMAC-SHA-1
- AES Known Answer Test (KAT)

A self-test failure causes an error to be logged to the RHEL system log. The module will enter an error state and be unloaded. While in an error state, the module inhibits all data output and does not provide any cryptographic functionality until the error state is cleared. Status output of the power-up self-tests is logged to the RHEL system log and the /proc filesystem entry "/proc/crym", which can be reviewed by the Crypto-Officer.

2.10 Design Assurance

Raytheon Oakley utilizes Subversion for its version control system. Raytheon Oakley maintains a unique branch for each major release and on occasion creates branches for special or experimental releases. The FIPS-specific version under evaluation is the current version with strict controls on any modification. Raytheon Oakley maintains all project software, configuration files, documentation, third party software, and third party binary executables within its configuration management system.

Additionally, Microsoft Visual SourceSafe (VSS) version 6.0 is used to provide configuration management for the module's FIPS documentation. Visual SourceSafe provides access control, versioning, and logging.

This Security Policy describes the secure operation of the FIPS Linux Cryptographic Module, specifies the procedures for secure installation, initialization, startup, and operation of the module, and provides guidance for use by Crypto-Officers and Users.

2.11 Mitigation of Other Attacks

This section is not applicable. The module does not claim to mitigate any attacks beyond the FIPS 140-2 Level 1 requirements for this validation.

3 Secure Operation

The Raytheon Oakley Systems FIPS Linux Cryptographic Module meets the Level 1 requirements for FIPS 140-2. The sections below describe how to ensure that the module is operating securely.

3.1 Initial Setup

The module requires no set-up, as it only executes in a FIPS-Approved mode of operation. When the module is powered up, it runs the power-on self-tests. If the power-up self-tests pass, the module is deemed to be operating in FIPS mode.

3.1.1 Installation

The module runs on a standard GPC. The module is pre-installed on the target platform at the factory, and requires no further actions from the customer in order for the module to execute as documented.

3.1.2 Management

No specific management activities are required to ensure that the module runs securely; the module only executes in a FIPS-Approved mode of operation.

3.2 Crypto-Officer Guidance

The Crypto-Officer can initiate the execution of self-tests, and can access the module's status reporting capability. Self-tests can be initiated at any time by reading the /proc filesystem entry /proc/crym. Status is reported automatically at the completion of the self-test execution.

3.3 User Guidance

The User accesses the module's cryptographic functionality. The User must not attempt to modify the configuration of the module as established by the Crypto-Officer, nor should a User reveal any of the CSPs used by the module to other parties.

4 Acronyms

Table 6 – Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
AGP	Accelerated Graphics Port
API	Application Programming Interface
BIOS	Basic Input/Output System
CBC	Cipher Block Chaining
CD-ROM	Compact Disc – Read-Only Memory
CMVP	Cryptographic Module Validation Program
CPU	Central Processing Unit
CSEC	Communications Security Establishment Canada
CSP	Critical Security Parameter
DVR	Digital Video Player
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FCC	Federal Communications Commission
FIPS	Federal Information Processing Standard
GPC	General Purpose Computer
HDD	Hard Disk Drive
HMAC	(Keyed-) Hash Message Authentication Code
IDE	Integrated Drive Electronics
IEEE	Institute of Electrical and Electronics Engineers
I/O	Input/Output
ISA	Industry Standard Architecture
KAT	Known Answer Test
MAC	Message Authentication Code
NIST	National Institute of Standards and Technology
OS	Operating System
PC	Personal Computer
PCI	Peripheral Component Interconnect
RHEL	Red Hat Enterprise Linux
SHA	Secure Hash Algorithm
UART	Universal Asynchronous Receiver/Transmitter
USB	Universal Serial Bus
VSS	Visual SourceSafe