Security Policy

Check Point CryptoCore version 2.0

FIPS 140-2

Level 1 Validation

Document Version 2.08

June, 2013

Table of Contents

Introduction 3
Purpose 3
References 3
Acronym list 3
Overview 4
Cryptographic Module 4
Module Ports and Interfaces 4
Roles, Services and Authentication 5
Physical Security 5
Operational Environment 5
Cryptographic Key Management 6
Self-Tests 6
Design Assurance 7
Mitigation of Other Attacks 7
Operation of the Check Point CryptoCore 2.0 7

Introduction

Purpose

This non-proprietary Cryptographic Module Security Policy for the Check Point CryptoCore 2.0, describes how the Check Point CryptoCore meets the Level 1 security requirements of FIPS 140-2. Validation testing was performed on Check Point 16-bit pre-boot. This policy document is part of FIPS 140-2 validation of the Check Point CryptoCore 2.0.

FIPS 140-2 (Federal Information Processing Standards Publication 140-2 Security Requirements for Cryptographic Modules) details the U.S. Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the NIST website at http://csrc.nist.gov/groups/STM/cmvp/index.html.

References

This document deals only with operations and capabilities of the Check Point CryptoCore 2.0 in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the Check Point CryptoCore 2.0 application from the following source:

Refer to: http://www.checkpoint.com for information on Check Point products and services as well as answers to technical or sales related questions.

Acronym list

Acronym	Definition
Triple-DES	Triple Data Encryption Standard
AES	Advanced Encryption Standard

Table 1 Acronyms

Overview

The Check Point CryptoCore 2.0 (hereinafter referenced as the crypto module) provides cryptographic support for the Check Point line of products. The crypto module is used to perform cryptographic operations as well as create, manage and delete cryptographic keys.

The cryptographic services provided by the crypto module in 16-bit encompasses symmetric encryption algorithms.

The crypto module can be used to provide multiple security functions in Check Point applications. A structured set of APIs can be called to perform these functions. The API set makes the module very flexible, and enables adding crypto functions to new applications without changing the module itself.

Utilizing the crypto module, Check Point applications can create encryption keys, which can then be used to encrypt data. The APIs provide the ability to encrypt both static data (such as hard disk blocks) as well as data streams (such as browser traffic).

The module is validated as documented in Table 2 below.

Security Section	Level
Cryptographic Module Specification	1
Cryptographic Module Ports and Interfaces	1
Roles, Services, and Authentication	1
Finite State Model	1
Physical Security	N/A
Operational Environment	1
Cryptographic Key Management	1
EMI/EMC	3
Self-Tests	1
Design Assurance	1
Mitigation of Other Attacks	N/A
Overall	1

Table 2 Security levels

Cryptographic Module

The Check Point CryptoCore 2.0 is classified as a multi-chip standalone module for FIPS 140-2 purposes. The module was tested for FIPS validation on a GPC running Check Point 16-bit pre-boot mode configured in single user mode. For exact details on tested platforms refer to the algorithm certificates listed in Table 5. Compliance is maintained for the above-mentioned operating system platforms on which the binary executable is unchanged.

The 16-bit Cryptographic Module is packaged in the form of a 16-bit binary in COM (MS-DOS) format that operates in the Pre-Boot environment.

The 16-bit module provides cryptographic functions during 16-bit operation in the Check Point Full Disk Encryption pre-boot application that serves to transparently encrypt/decrypt data on block I/O devices such as hard disks.

Module Ports and Interfaces

The Check Point CryptoCore 2.0 is classified as a multi-chip standalone module for FIPS 140-2 purposes. As such, the module's cryptographic boundary includes the following:

- CheckPoint PreBoot: ccore16.bin

A PC or mobile device running an operating system and interfacing with the computer, keyboard, mouse screen, floppy drive, CD-ROM drive, speaker, serial ports, parallel ports, and power plug.

The Check Point CryptoCore 2.0 provides a logical interface via an Application Programming Interface (API). The API provided by the module is mapped to the FIPS 140-2 logical interfaces: data input, data output, control input, and status output. All of these physical interfaces are separated into the logical interfaces from FIPS as described in the following table:

FIPS 140-2 Logical Interface	Module Mapping
Data Input Interface	Parameters passed to the module via the API call
Data Output Interface	Data returned by the module via the API call
Control Input Interface	Control input through the API function calls
Status Output Interface	Information returned via exceptions and calls
Power Interface	Does not provide a separate power or maintenance access interface beyond the power interface provided by the computer itself

Table 3 FIPS 140-2 Logical Interfaces

Roles, Services and Authentication

The cryptographic module provides Crypto Officer and User roles. All the services exported by the module are common to both the roles except key zeroization. Only the Crypto-officer is allowed to perform key zeroization. Since the module is validated at security level 1, it does not provide an authentication mechanism.

Exported Services	Exported to
cryptInitSystem	User/CO
cryptCipherDestroy	CO
cryptCipherSetParams	User/CO
cryptCipherSetKey	User/CO
cryptCipherSetIV	User/CO
cryptCipherGetIV	User/CO
cryptEncrypt	User/CO
cryptDecrypt	User/CO
cryptXTSEncrypt	User/CO
cryptXTSDecrypt	User/CO
cryptGetStatusInfo	User/CO
cryptEnableAesCpuAcceleration	User/CO

Table 4 Exported Functions

Physical Security

Since the Check Point Crypto Module is implemented solely in software, the physical security section of FIPS 140-2 is not applicable.

Operational Environment

The Cryptographic module's software components are designed to be installed on the targets listed below as indicated in section Cryptographic Module above.

16-Bit Pre-boot module

The 16-bit cryptographic module's software components are designed to be used on an IBM-compatible PC with BIOS pre-boot environment. An operating system is not required for the pre-boot module. The BIOS based pre-boot module was tested on an Dell Latitude E6500 (Intel CoreT2 Duo CPU T9800 2.93 GHz) and an Apple Macbook Pro (Intel Core i7 2.4 GHz with AES-NI).

Each software components of the module will implement an approved message authentication code, used to verify the integrity of software component during the power-up self-test (see section on self-test below). While loaded in the memory, the respective target OS will protect all unauthorized access to the Cryptographic module's address memory and process space.

Cryptographic Key Management

The Check Point CryptoCore 2.0 implements the following algorithms.

Algorithm Type	Algorithm, Modes and Key length	FIPS Approved	Algorithm Certificate #
Symmetric Key	AES - ECB, CBC, XTS – 128, 192, 256 Triple-DES – ECB, CBC – 168	Yes Yes	2181 1381

Table 5 Algorithms list

The following table provides a list of keys and key sizes that can be generated and/or used with the module. Keys are generated or inserted, i.e. provided as input to the data input interface of the service (API), as specified in the API listing. See Table 7 for details of how the critical security components (CSP) are inserted into, or generated by, the module.

Key Name	Created	Size(s) in bits	Purpose
AES_key	Inserted	128, 192, 256,	Encryption, Decryption
Triple-DES_key	Inserted	192 (168)	Encryption, Decryption
Triple-DES_MAC_MIT_key	Hard-coded	192 (168)	Module Integrity Testing

Table 6 List of Keys/CSPs

Type	Algorithms	Service	CSP	Inserted/ Generated	Access Type
Initialization	N/A	cryptInitSystem	N/A	N/A	N/A
Symmetric Cipher					
	AES, Triple-DES	cryptCipherDestroy	Secret Key	Inserted	Write
		cryptCipherSetParams	Secret Key	Inserted	Read
		cryptCipherSetKey	Secret Key	Inserted	Read
		cryptCipherSetIV	N/A	N/A	N/A
		cryptCipherGetIV	N/A	N/A	N/A
		cryptEncrypt	Secret Key	Inserted	Read
		cryptDecrypt	Secret Key	Inserted	Read
		cryptXTSEncrypt	Secret Key	Inserted	Read
		cryptXTSDecrypt	Secret Key	Inserted	Read
Non FIPS Validated Services					
Retrieve function pointers		cryptGetFunctionList	N/A	N/A	N/A
Get module info		cryptGetStatusInfo	N/A	N/A	N/A
Disable/Enable AES-NI		cryptEnableAesCpuAcceleration	N/A	N/A	N/A

Table 7 Key/CSP Access

When keys are set for deletion, the key is zeroized by overwriting the keys to ensure it cannot be retrieved. Zeroization is done by calling the cryptCipherDestroy() service. Sensitive intermediate data is zeroized by the module itself.

Self-Tests

The Check Point CryptoCore 2.0 performs several power-up self-tests including known answer tests for the FIPS Approved algorithms listed in the table below.

The crypto module also performs a self-test integrity check using Triple-DES-MAC with a fixed key to verify the integrity of the module.

Algorithm	Power-up self-test	Conditional self test

AES KAT	Yes (encrypt/decrypt)	N/A
Triple-DES KAT	Yes (encrypt/decrypt)	N/A

Table 8 List of Self tests

Design Assurance

Check Point maintains versioning for all source code and associated documentation through CVS versioning handling system.

Mitigation of Other Attacks

The Check Point CryptoCore 2.0 does not employ security mechanisms to mitigate specific attacks.

Operation of the Check Point CryptoCore 2.0

The Check Point CryptoCore 2.0 is designed for installation and use on a computer configured in single user mode, and is not designed for use on systems where multiple, concurrent users are active.

AES (Cert. #2182, key wrapping; key establishment methodology provides between 128 and 256 bits of encryption strength).