Kernel NPX Cryptographic Module

FIPS 140-2 Non-Proprietary Security Policy

Adara Networks, Inc.

Document Name: Kernel NPX Cryptographic Module FIPS 140-2 Non-Proprietary Security Policy

Document Version: 1.6

Revision Date: December 1, 2010

CHANGE RECORD

Revision	*Date*	*Author*	
1.0	3/16/10	Jerry Toung	Preliminary version for all platforms
1.2	3/16/2010	Patrick Mahan	Editoral changes
1.3	3/17/10	Patrick Mahan	Review Version
1.4	3/17/10	Patrick Mahan	Final Version
1.5	7/7/10	Patrick Mahan	Submission Version
1.6	12/01/10	Patrick Mahan	Updated Sections 1 and 8

Contents

Tables

Figures

1 Module Overview

The Adara Networks Kernel NPX Cryptographic Module (SW Version 1.0) (hereafter the Module) for FreeBSD is a software module implemented as a shared library (crypto-fips.ko). When loaded into computing system memory, it resides at the kernel mode level of the FreeBSD Operating System and enables and enforces an assortment of FIPS approved cryptographic services accessible to other kernel subsystems.

For FIPS 140-2 purposes, the cryptographic module is classified as a multi-chip standalone module.

The Module is designed and implemented to meet the Level 1 requirements of FIPS publication 140-2 under the FreeBSD 8.0 operating system.

The cryptographic module was tested on the following platforms:

- HP DL 360 G5 platform with an Intel Xeon E5440 processor with a FreeBSD 8.0 system (single-user mode)

- Radisys ATCA-4500 platform with an Intel Xeon L5518 processor with a FreeBSD 8.0 system (single-user mode)

The module supports the FIPS Approved AES, Triple-DES (TDES), SHA-1 and HMAC-SHA-1 algorithms.

Figure 1 depicts the logical block diagram for the module, with the cryptographic boundary shown in red.

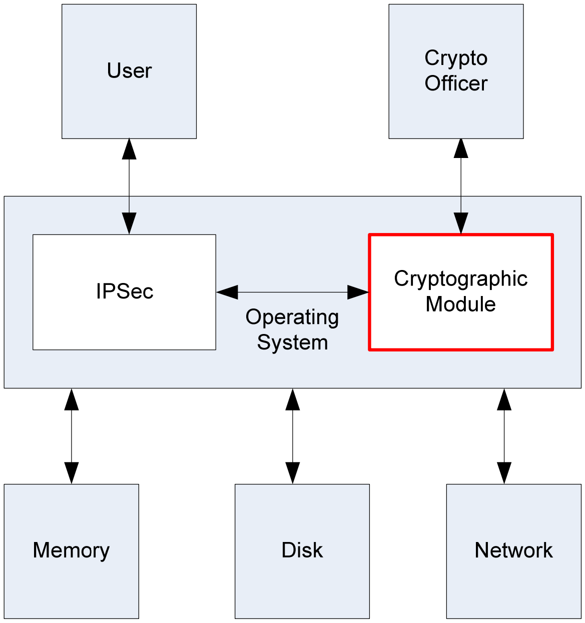

Figure 1 - Logical Block Diagram

All the cryptographic services made available by the Module are available only to operating system kernel mode subsystems, which are a part of kernel memory. The operating system, acting on behalf of end-users, is the operator of the module.

2 Security Level

The cryptographic module meets the overall requirements applicable to Level 1 security of FIPS 140-2.

Since the cryptographic module does not support asymmetric cryptographic methods, no special effort was taken to mitigate side-channel attacks, in particular those based on timing and power analysis and fault induction.

Table 1 - Module Security Level Specification

	Level
Cryptographic Module Specification	1
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	1
Self-Tests	1
Design Assurance	1
Mitigation of Other Attacks	N/A

3 Modes of Operation

The Module does not support a non-Approved mode of operation.

3.1 FIPS Approved Mode of Operation

The cryptographic module is known to be in FIPS mode if and only if the global system control variable (security.bsd.fips_mode) is set to “1”. If this value is not “1” then the FIPS compliant kernel cryptographic module will fail to load and an error will be generated.

In FIPS mode, the cryptographic module only supports FIPS Approved algorithms as follows:

- Kernel AES 128 CBC mode (Cert. #1410)
- Kernel Triple-DES - TCBC mode (Cert. #963)
- Kernel SHA-1 for data hashing (Cert. #1280)
- Kernel HMAC-SHA-1 for MAC computation and verification based on FIPS PUB 198 (Cert. #831)

4 Ports and Interfaces

All FIPS ports and interfaces are defined and contain all data input, data output, control input, and status output interfaces to and from the module. The physical ports of the module are the same as the computer system on which it is executing. The logical interface is the modules application program interface (API).

The Data input and output interface consists of the input and output parameters defined by the API functions. The Control input interface defined by the API functions called and the Status output interface includes the values returned from the API functions.

5 Identification and Authentication Policy

5.1 Assumption of Roles

The single operator of the module is defined as the Operating System (OS). The cryptographic module shall support two operator roles, the User, and the Cryptographic-Officer (CO). The cryptographic module does not provide an authentication mechanism.

Table 2 - Roles and Required Identification and Authentication

Role	Description	Authentication Type	Authentication Data
CO	Installs the module and configures the system to load the correct version. This role has access to all of the services provided by the cryptographic module.	N/A	N/A
User	This role may have access to all of the services provided by the cryptographic module via the IPSEC protocol. Service access is dependent upon Cryptographic Officer.	N/A	N/A

Table 3 - Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
Not Applicable	Not Applicable

6 Access Control Policy

6.1 Roles and Services

Table 4 - Services

Cryptographic Officer	Module Initialization
	AES encryption and decryption
	TDES encryption and decryption
	Generate Keyed Hash
	Generate Message Digest
	Show Status
	Self-tests
	Zeroize
User	AES Encryption and Decryption
	TDES Encryption and Decryption
	Generate Keyed Hash
	Generate Message Digest
	Show Status
	Self-tests
	Zeroize

6.2 Definition of Critical Security Parameters (CSPs)

The module contains the following CSPs:

Table 5 - CSPs

CSP	Description	Generation	Storage	Establishment	Access
Symmetric Keys	AES 128-bit key, Triple DES 112 or 192 bit key for encryption / decryption	External generation	Storage: RAM plaintext	Agreement: NA Entry: NA Output: NA	Crypto Officer/User R W D
HMAC Secrets	160-bit HMAC SHA1 for message authentication and integrity	External generation	Storage: RAM plaintext	Agreement: NA Entry: NA Output: NA	Crypto Officer/User R W D

7 Operational Environment

The following operational rules must be followed by any user of the Module:

- Virtual memory of the computing system must be configured to reside on a local storage device.
- It is the responsibility of the CO to configure the system to operate securely and, whenever it is necessary, to prevent remote login.

8 Security Rules

The cryptographic module's design corresponds to the cryptographic module's security rules. This section documents the security rules enforced by the cryptographic module to implement the security requirements of this FIPS 140-2 Level 1 module.

When the OS loader attempts to load the Module into memory, the Module runs an integrity test and a number of cryptographic functionality self-tests. If all the tests pass successfully, the Module makes a transition to Utilization state when the API calls can be used by other kernel subsystems to carry out desired cryptographic services. Otherwise, the Module returns to Soft Error state and the OS reports failure of the attempts to load it into memory.

1. The cryptographic module is not required to provide authentication of the operator to access roles and services.
2. Roles are implicitly applied.
3. The cryptographic module shall perform the following tests:
   A. Power up Self-Tests:
      1. Power-on self-tests are run upon every initialization of the module and if any of the tests fail, the process will be halted and the module will not initialize. In this error state, no services can be accessed by the users. The module implements the following power on self-tests:
         - AES KATs
         - SHA-1 KAT
         - HMAC-SHA-1 KAT
         - Triple-DES KAT
      2. Integrity Test. The software integrity test computes a HMAC-SHA-1 value by applying the digest calculation to the entire kernel cryptographic loadable module. The test fails if the value computed on the image of the Module does not match the original value computed by the vendor and stored inside the Module.
4. The error state is indicated by the return of "invalid argument".
5. Data output shall be inhibited during power-up self-tests and error states. If any component of the power up self-test fails the module shall enter an error state and prevent all cryptographic processing. The module may be reinitialized to recover from the error state.
6. The module shall perform the power-up self-tests without requiring any operator intervention.
7. At any time the cryptographic module is in an idle state, the operator shall be capable of commanding the module to perform the power-up self-test by reinitializing the module.
8. Status information shall not contain CSPs or sensitive data that if misused could lead to a compromise of the module.

This section documents the security rules imposed by the vendor:

1. The module shall only operate in the approved mode of operation.
2. The module shall not provide cryptographic services prior to initialization of the module.
3. The module itself shall not provide a method for porting CSPs into or out of the physical boundary.

9 Physical Security Policy

The FIPS 140-2 Area 5 Physical Security requirements are not applicable because the module is software only.

10 Mitigation of Other Attacks Policy

The module has not been designed to mitigate any specific attacks.

11 References

[FIPS 140-2] FIPS Publication 140-2 *Security Requirements for Cryptographic Modules*

[FIPS 198] The Keyed-Hash Message Authentication Code

12 Definitions and Acronyms

AES	Advance Encryption Algorithm
API	Application Programming Interface
CBC	Cipher Block Chaining
CSP	Critical Security Parameter
EMI/EMC	Electromagnetic Interference/ Electromagnetic Compatibility
FIPS	Federal Information Processing Standard
HMAC	Hash Message Authentication Code
IPSEC	Internet Protocol Security
KAT	Known Answer Test
OS	Operating System
RAM	Random Access Memory
SHA	Secure Hash Algorithm
TDES	Triple – Data Encryption Standard