NSM Application Cryptographic Module

Security Policy

Version: 1.9

Revision Date: May 28, 2014

CHANGE RECORD

Revision	***Date***	***Author***	***Description of Change***
1.0	11/13/2009	James Reardon	Initial version
1.1	11/23/2009	James Reardon	Added Algorithm Cert #’s
1.2	12/9/2009	James Reardon	Updated TBDs
1.3	4/01/2010	James Reardon	Updated Table 3
1.4	10/12/2012	James Reardon	Updates for v2.0
1.5	2/21/2013	James Reardon	Updates to address Lab comments
1.6	3/15/2013	James Reardon	More updates per Lab comments
1.7	5/22/2013	James Reardon	Updates after Op Test; accepted all tracked changes
1.8	2/18/2014	James Reardon	Updates to address CMVP comments.
1.9	5/28/2014	James Reardon	Updates to address CMVP comments.

Contents

Tables

Figures

1 Module Overview

McAfee Network Security Platform is a network-class IPS appliance that protects every network-connected device by blocking attacks in real time before they can cause damage. It combines IPS, application control, and behavioral detection to block encrypted attacks, botnets, SYN flood, DDoS, and Trojans and enable regulatory compliance. It protects business, systems, and networks with one proven solution that goes beyond IPS. The NSM Application Cryptographic Module provides cryptographic services for the Network Security Manager application.

The McAfee NSM Application Cryptographic Module is a software module designed to operate in compliance with FIPS 140-2 Level 1 security requirements.

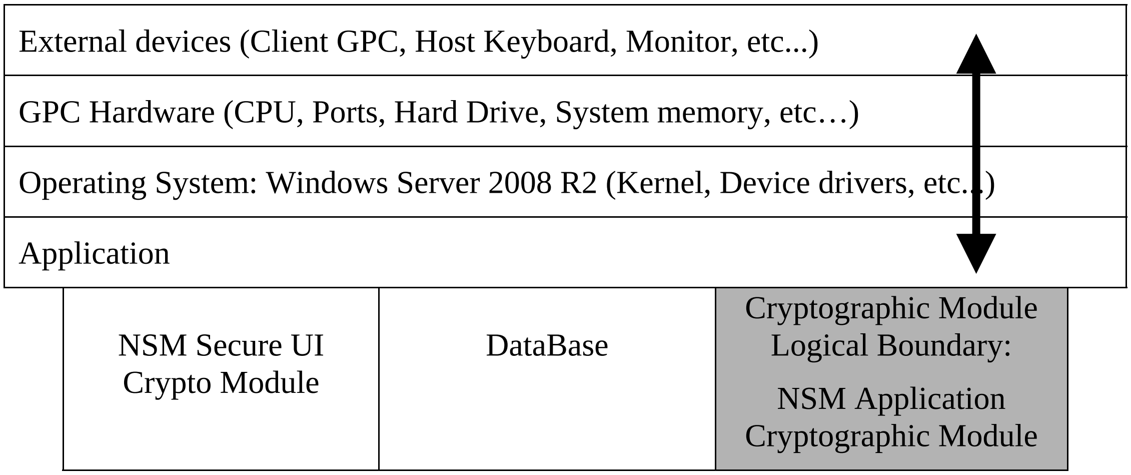
External devices (Client GPC, Host Keyboard, Monitor, etc...)
GPC Hardware (CPU, Ports, Hard Drive, System memory, etc…)
Operating System: Windows Server 2008 R2 (Kernel, Device drivers, etc…)
Application
NSM Secure UI Crypto Module
DataBase
Cryptographic Module Logical Boundary:
NSM Application Cryptographic Module

Figure 1 –Cryptographic Module Diagram

The logical boundary of the module is defined by the configuration software for this validation is:

Software: NSM Application Cryptographic Module
Software Version: 7.1.15.1.11
Embedded Library: RSA BSAFE Crypto-J 6.1.0.0.2

Security Level

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

Table 1 - Module Security Level Specification

Security Requirements Section	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	3
Self-Tests	1
Design Assurance	3
Mitigation of Other Attacks	N/A

2 Modes of Operation

2.1 FIPS Approved Mode of Operation

The module operates in the Approved mode of operation following successful power up initialization, configuration and adherence to security policy rules and requirements. Rules and requirements for operation in the approved mode of operation are defined in Sections 6 and 7.

It is the responsibility of the operator of the module to ensure that algorithms, modes, and key sizes Disallowed per NIST SP 800-131A are not used (see Section 2.2 below).

The cryptographic module supports the following FIPS Approved algorithms.

Table 2 - FIPS Approved Algorithms Used in Current Module

FIPS Approved Algorithm	CAVP Cert. #
BSafe TLSv1: AES – 128 and 256 bits CBC and CFB	2469
BSafe TLSv1: RSA Verify 1024 bits	1259
BSafe TLSv1 and elsewhere: SHA-1, SHA-256, and SHA-512	2083
Bsafe TLSv1 and elsewhere: RNG FIPS 186-2 –SHA-1 G function.	1198
BSafe TLSv1 and elsewhere: HMAC-SHA-1	1513
BSafe TLSv1: SP 800-135 KDF – TLS 1.0/1.1 *This protocol has not been reviewed or tested by the CAVP and CMVP.*	78 (CVL)

The cryptographic module supports the following non-FIPS Approved algorithms which are allowed for use in FIPS mode.

Table 3 - Non-FIPS Approved Algorithms Allowed in FIPS Mode

FIPS Allowed Algorithms
Bsafe TLSv1: MD5 and HMAC-MD5 within the TLS protocol. Not to be used with cipher-suite.
BSafe Non-Approved RNG: Seeding source for the FIPS 186-2 RNG, with 140 bits of min-entropy. The module generates cryptographic keys whose strengths are modified by available entropy.

2.2 Non-Approved Mode of Operation

The cryptographic module supports the following algorithms which are Disallowed as of January 1, 2014 per the NIST SP 800-131A algorithm transitions:

Table 4 – Algorithms Disallowed per NIST SP 800-131A Transitions

Disallowed Algorithms
BSafe RSA 1024 bit Encryption for key establishment, the key transport method provides 80 bits of security strength (non-compliant).

Algorithms providing less than 112 bits of security strength (Disallowed per NIST SP 800-131A) are not allowed in the FIPS Approved mode of operation for use by Federal agencies.

The following CSPs, public keys and services are affected if the above listed Disallowed algorithms are used (see Section 5):

CSPs

- Sensor Upload/Download Key
- NSM Private Key for Sensor Communication
- NSM Session Keys – Confidentiality
- NSM Session Keys – Integrity
- NSM Session Key – Shared Secret

Public Keys

- Sensor Public Key

Services

- GPC/OS System Administration services
- Security Admin Services / Super-User – UI interface
- Sensor Management Service
- Request Sensor Update

Note: This section and the non-Approved mode were added to the Security Policy retroactively in 2014 due to SP 800-131A transitions and CMVP guidelines. This is strictly a documentation update.

3 Ports and Interfaces

The cryptographic module is a multi-chip standalone embodiment consistent with a GPC with ports and interfaces as shown below.

Table 5 - FIPS 140-2 Ports and Interfaces

Physical Port	Logical Interface	FIPS 140-2 Designation	Interface Name and Description
Power	None	Power Input	GPC, Power Supply
Ethernet	Application Programming Interface (API)	Data Input/Data Output, Control Input, Status Output	Logical TCP, UDP over IP Supports HTTP, SNMPv3, v2(read only), v1(read only), HTTPS, TLS
Serial	None	Control Input	GPC, no logical support
Mouse	API	Data Input, Control input	GPC, control input and data via cut and paste.
Keyboard	API	Data Input, Control Input	Keyboard signals input Logical data and control entry
LED	None	Status Output	GPC: no logical support
Video	API	Data Output, Status Output	Output of visual display signals for data and status

4 Identification and Authentication Policy

4.1 Assumption of Roles

The module supports three distinct operator roles: User, Cryptographic Officer (CO), and Sensor. The cryptographic module enforces the separation of roles using Apache Session IDs.

Table 6 - Roles

Role	Description
CO	This role has access to all services offered by the module through the product's User Interface. This role includes the GPC/OS System Admin and NSM Super user.
User	This role has access to all services offered by the module. n.b. The User role may have access to all NSM services provided to the CO. This will be determined by the privileges assigned by the CO to the User.
Sensor	This role has the ability to provide status to NSM.

5 Access Control Policy

5.1 Roles and Services

Table 7 – Authorized Services

CO	User*	Sensor	Service	Description
X	X		GPC/OS System Administration services	Maintain System and OS And Ensure FIPS compliant configuration of the Operational environment.
X	X		Security Admin Services Super-User – UI interface	Configure and operate NSM Application.
X	X		UI Logout	Logout and terminate UI session.
X	X		Sensor Management Service	Push configuration, attack signatures, and firmware updates to sensor. Reboot, Pull Status, pull sensor logs, Profiling Information.
X	X		Update Server service	Obtain attack signatures, firmware updates for sensor modules from Update server
		X	Request Sensor Update	Obtain attack signatures and configuration data from NSM.

(*) – The User's available services are defined by the Cryptographic Officer (CO). The CO may allocate all services to all Users as indicated here, however this is the discretion of the CO.

5.2 Other Services

The following services are available to any operator without assuming an authorized role:

- Self-Tests (initiated by reloading the module into memory)
- Get Status
- Zeroization
- Communication with MySQL

5.3 Definition of Critical Security Parameters (CSPs)

The module contains the following CSPs:

Table 8 - Private Keys and CSPs

Key/CSP Name	Description	Algorithm
Sensor Upload/Download Key	Bulk transfer channel to the sensor.	AES 128 CFB
NSM Private Key for Sensor Communication	Authenticates NSM server to sensor in TLS.	RSA 1024
Sensor INIT Communication Shared Secret Password	Password used to authenticate the Sensor to an application Server. Both sides generate a challenge and verify existence of shared secret.	CHAP-SHA-1 comparison
NSM Session Keys - Confidentiality	TLS session derived keys for encryption/decryption	AES 128 CBC
NSM Session Keys - Integrity	TLS session derived keys for integrity	HMAC-SHA-1
NSM Session Key – Shared Secret	TLS pre-master secret used to derive session keys	Used by TLSv1 KDF
BSafe Seed/Seed key	RNG State	Used by FIPS 186-2 RNG

5.4 Definition of Public Keys

The module contains the following public keys:

Table 9 - Public Keys

Key Name	Type	Description
Sensor Public Key	RSA 1024	Wraps and authenticates the Sensor upload/download key
NSM Public Sensor Communication Key	RSA 1024	Used to Authenticate the Server to the Sensor in TLS.

5.5 Definition of CSPs Modes of Access

Table 10 defines the relationships between role access to CSPs and the different module services. The modes of access shown in the table are defined as:

- **G** = Generate: The module generates the CSP.
- **E** = Execute: The module uses the CSP.
- **R** = Read: Export of the CSP.
- **W** = Write: Import/Establishment of CSP.
- **Z** = Zeroize: The module zeroizes the CSP.

Table 10 - CSP Access Rights within Roles & Services

Role	Authorized Service	Mode	Cryptographic Key or CSP
User, CO	GPC/OS System Administration services	R, W, Z	All CSPs
User, CO	Security Admin Services Super-User – UI interface	G, E, W	NSM Session Key - Confidentiality
		G, E, W	NSM Session Key - Integrity
		G, E, W	NSM Session Key – Shared Secret
User, CO	UI Logout	N/A	N/A
User, CO	Sensor Management Service	E	Sensor Upload/Download Key
		E	NSM Private Key for Sensor Communication
		E, W	Sensor INIT Communication Shared Secret Password
User, CO	Update Server Service	N/A	N/A
Sensor	Request Sensor Update	G	Sensor Upload/Download Key

6 Operational Environment

The operational environment requires the following configuration process:

1. Server grade, General Purpose Computing Platform, with Intel Core 2 Quad processor.
2. Configure Windows Server 2008 R2 for the following access control settings:
    a. Set Minimum Password Length = 8
    b. Set Account Lockout Threshold = 5
    c. Set Account Lockout Duration = 30 minutes
    d. Enable Audit of following Audit Types:
        - Information
        - Warning
        - Error
        - Success Audit
        - Failure Audit
3. Install NSM Package, Configure super user and user access policies per authentication strength requirements. Select install for FIPS mode.
4. Managed Sensors must be running in FIPS mode.

7 Security Rules

1. When the module has not been placed in a valid role, the operator shall have limited access to cryptographic security functions.
2. The cryptographic module shall perform the following tests

   A. Power up Self-Tests

      1. Cryptographic algorithm tests
         a. AES Encrypt and Decrypt Known Answer Test
         b. SHA-1 Known Answer Test (performed during HMAC-SHA-1 and TLSv1 KDF KATs)
         c. HMAC-SHA-1 Known Answer Test (per FIPS IG 9.1, performed during Software Integrity Test)
         d. RNG, FIPS 186-2 – SHA-1 Based Known Answer Test
         e. RSA Verify Known Answer Test
         f. RSA Encrypt/Decrypt Known Answer Test
         g. TLSv1 KDF Known Answer Test
      2. Software Integrity Test - HMAC-SHA-1

   B. Conditional Self-Tests

      1. Continuous Random Number Generator (RNG) test
         a. Non Approved RNG (per FIPS IG 9.8, this is not performed if RNG only seeded once)
         b. Approved RNG - FIPS 186-2

3. Failure of self-tests will cause the module to transition to a FIPS error state. Logical components will shut-down and no data output will be provided during error states.
4. The operator shall be capable of commanding the module to perform the power-up self-test by cycling power or resetting the module.
5. Power-up self tests do not require any operator action.
6. Data output shall be inhibited during self-tests and error states.
7. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
8. The module ensures that the seed and seed key inputs to the Approved RNG are not equal.
9. There are no restrictions on which keys or CSPs are zeroized. Zeroization shall be performed by the Cryptographic Officer by uninstalling the application, formatting the hard drive and power cycling the device. The cryptographic officer shall directly observe the completion of this process.
10. The module does support concurrent operators.
11. The module does not support a maintenance interface or role.
12. The module does not support manual key entry.
13. The module does not output intermediate key values.

14. The module shall support SNMPv1, v2, v3 for status output to third party network management systems. There is no claim of security strength associated with these protocols and all communications are considered clear-text.
15. The module shall support SNMP v3 communication to Sensors. There is no claim of security strength associated with these protocols and all communications are considered clear-text.
16. TLSv1 must be negotiated with encryption and integrity using the following ciphersuite: TLS_RSA_WITH_AES_128_CBC_SHA.
17. The “SSL Decryption” service shall be disabled.

8 Physical Security Policy

8.1 Physical Security Mechanisms

The cryptographic module is a software only module. Physical Security for the GPC is not Applicable to the requirements of FIPS 140-2.

9 Mitigation of Other Attacks Policy

The module has not been designed to mitigate attacks which are outside of the scope of FIPS 140-2.

10 References

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

11 Acronyms

API	Application Programming Interface
IPS	Intrusion Prevention System