NSM Application Cryptographic Module

Security Policy

Version: 1.3

Revision Date: April 1, 2010

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

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 Crypto 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 2 security requirements.

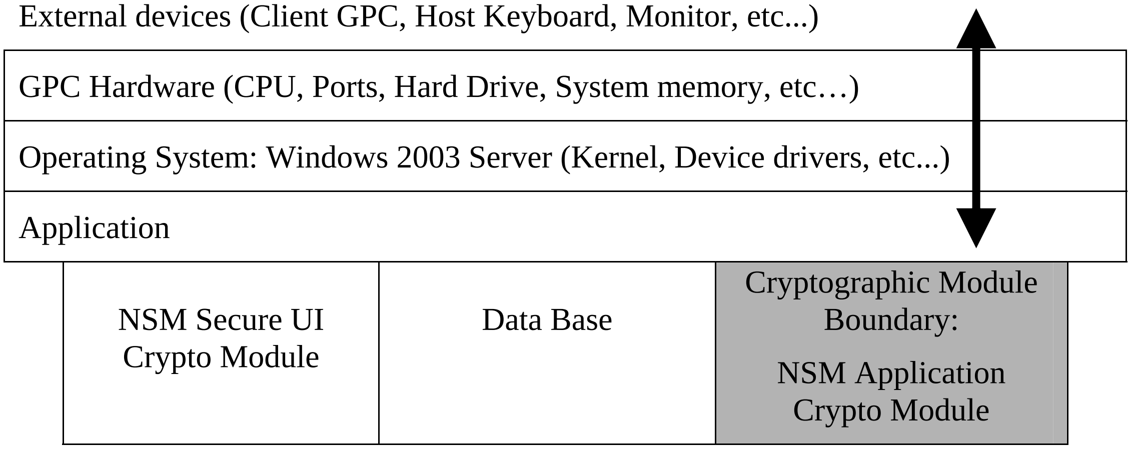
External devices (Client GPC, Host Keyboard, Monitor, etc...)
GPC Hardware (CPU, Ports, Hard Drive, System memory, etc…)
Operating System: Windows 2003 Server (Kernel, Device drivers, etc...)
Application
NSM Secure UI Crypto Module
Data Base
Cryptographic Module Boundary:
NSM Application Crypto Module

Figure 1 –Cryptographic Module Diagram

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

Software: NSM Application Cryptographic Module
Software Version: 1.0
Available in the following: McAfee NSM 5.1 Cryptographic Module Package, Version 5.1.15.10

The module was operational tested on the following Common Criteria evaluated platform:

- Dell PowerEdge SC1420 running Windows Server 2003 Standard (SP 2)
  CC EAL 4
  CCEVS Validation Report available at:
  http://www.niap-ccevs.org/st/st_vid10184-vr.pdf

The system patches and updates configured as described in the OS Security Target (http://www.niap-ccevs.org/cc-scheme/st/st_vid10184-st.pdf)

Security Level

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

Table 1 - Module Security Level Specification

Security Requirements Section	Level
Cryptographic Module Specification	2
Module Ports and Interfaces	2
Roles, Services and Authentication	2
Finite State Model	2
Physical Security	N/A
Operational Environment	2
Cryptographic Key Management	2
EMI/EMC	3
Self-Tests	2
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 section 6.

2.1.1 Approved and Allowed Algorithms

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 bits CBC and CFB	1237
BSafe TLSv1: RSA Verify 1024 bits	593
BSafe TLSv1 and elsewhere: SHA-1	1135
Bsafe TLSv1 and elsewhere: RNG FIPS 186-2 –SHA-1 G function.	684
BSafe TLSv1 and elsewhere: HMAC SHA-1	721

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 RSA 1024 bit Encryption for key establishment, the key transport method provides 80 bits of security strength.
Bsafe TLSv1: MD5 and HMAC-MD5 within the TLS protocol. Not to be used with cipher-suite.
BSafe Non-Approved RNG: seeding source

2.2 Non-Approved Mode of Operation

The module supports a Non-Approved mode of operation.

2.2.1 Non-Approved Algorithms

The cryptographic module supports the following non-Approved algorithms in the non-Approved mode of operation.

Table 4 - Non-Approved, Non-Allowed Algorithms

Non-Approved Algorithm
Bsafe TLSv1: DES, RC4
Bsafe TLSv1: MD5 and HMAC-MD5 cipher suite

3 Ports and Interfaces

The cryptographic module is a multichip standalone consistent with a GPC with ports and interfaces as shown below.

Table 5 - FIPS 140-2 Ports and Interfaces

Physical Port	FIPS 140-2 Designation	Interface Name and Description
Power	Power Input	GPC, Power Supply
Ethernet	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	Control Input	GPC, no logical support
Mouse	Data Input, Control input	GPC, control input and data via cut and paste.
Keyboard	Data Input, Control Input	Keyboard signals input Logical data and control entry
LED	Status Output	GPC: no logical support
Video	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 and Required Identification and Authentication

Role	Description	Authentication Type	Authentication Data
CO	This role has access to all services offered by the module		
	GPC/OS System Admin	Required to configure an 8 character password. 96 ascii chars are supported. The probability of guessing this value is 1 in 96^8, which is less than 1 in a 1,000,000. The OS allows 5 attempts per minute. The probability is 5 in 96^8 which is less than 1 in 100,000.	Username and Password
	NSM Super user	RSA 1024-bit signature verification. The authentication mechanism is based on 1024-bit RSA, which has a key strength of 80 bits. 80 bits provides a probability of 1/2^80 that a random attempt will succeed or a false acceptance will occur. This is far less than 1 in 1,000,000. The application allows 60,000 attempts per minute. The probability is 60,000/2^80 which is less than 1 in 100,000.	Digital Signature Verification
		The Shared Secret is 32 bytes in length (256 bits). The probability that a random attempt will succeed or a false acceptance will occur is 1/(2^256), which is less than 1 in a 1,000,000. The application allows 60 authentication attempts per minute. The probability is 60 in 2^256 which is less than 1 in 100,000	Shared Secret

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.	CAC: The probability is 1 in 2^80 which is less than 1 in 1,000,000. The application allows 60,000 attempts per minute. The probability is 60,000/ (2^80) which is less than 1 in 100,000.	Digital Signature Verification
		The Shared Secret is 32 bytes in length (256 bits). The probability that a random attempt will succeed or a false acceptance will occur is 1/(2^256), which is less than 1 in a 1,000,000. The application allows 60 authentication attempts per minute. The probability is 60 in 2^256 which is less than 1 in 100,000	Shared Secret
Sensor	Role has the ability to provide status to NSM app.	Required to configure an 8 character password. 96 ascii chars are supported. The probability of guessing this value is 1 in 96^8, which is less than 1 in a 1,000,000. The application allows 60 attempts per minute. The probability is 60 in 96^8 which is less than 1 in 100,000 Per signature strength. The probability is 1 in 2^80 which is less than 1 in 100,000. The application allows 60,000 attempts per minute. The probability is 60,000/ (2^80) which is less than 1 in 100,000.	Password: Used for the Initial authentication to the module prior to establishment of public certs. CHAP mutual. -OR- TLS- RSA 1024 Static. Self-signed cert. SHA-1 FIPS 140-2 sensor Communications v.01

5 Access Control Policy

5.1 Roles and Services

Table 7 – Authenticated 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. Zeroize
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. 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. The Crypto Officer may allocate all services to all users as indicated here, however this is the discretion of the Cryptographic Officer.

5.2 Unauthenticated Services

The cryptographic module provides unauthenticated access to status information, self-test initiation, and zeroization.

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	TFTP bulk transfer channel to the sensor.	AES 128 CFB
NSM private key for Sensor communication	Authenticates NSM server to sensor.	RSA 1024
Sensor INIT communication Shared Secret password	Password used to authenticate Sensor 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	TLSv1 KDF
BSafe Seed/Seed key	RNG State	FIPS 186-2 RNG
UI Shared Secret	Shared secret authentication data for UI communication	Authentication
CO’s OS System Administrator Password.	Authenticates operator to allow configuration and maintenance of System Software and OS.	Authentication

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
Sensor Update Verification Public Key	RSA 1024	Sensor firmware files, licensing files and attack signatures verification key for files transferred to server.
NSM Public Sensor Communication Key	RSA 1024	Used to Authenticate the Server to the Sensor.

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	E, W	NSM session Key - Confidentiality
		E, W	NSM session Key - Integrity
		E, W	NSM session Key – Shared secret
User, CO	UI Logout	E, R	UI Shared Secret
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. The module was operational tested on the following Common Criteria evaluated platform Dell PowerEdge SC1420 running Windows Server 2003 Standard (SP 2); CC EAL 4; CCEVS Validation Report available at: http://www.niap-ccevs.org/st/st_vid10184-vr.pdf. The system patches and updates shall be configured as described in the OS Security Target (http://www.niap-ccevs.org/cc-scheme/st/st_vid10184-st.pdf)
2. Configure the Windows 2003 Server 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. The cryptographic module shall provide role-based authentication.
2. The cryptographic module shall clear previous authentications on power cycle.
3. When the module has not been placed in a valid role, the operator shall have limited access to cryptographic security functions.
4. 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
         c. HMAC-SHA-1 Known Answer Test
         d. RNG, FIPS 186-2 – SHA-1 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
         b. Approved RNG - FIPS 186-2

5. Failure of self-tests will cause all module to transition to a FIPS error state. Logical components will shut-down and no data output will be provided during error states.
6. The operator shall be capable of commanding the module to perform the power-up self-test by cycling power or resetting the module.
7. Power-up self tests do not require any operator action.
8. Data output shall be inhibited during self-tests and error states.
9. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
10. The module ensures that the seed and seed key inputs to the Approved RNG are not equal.
11. 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.
12. The module does support concurrent operators.
13. The module does not support a maintenance interface or role.
14. The module does not support manual key entry.

15. The module does not output intermediate key values.
16. The module shall not be caused to share CSPs between the Approved and Non-Approved mode of operation.
17. 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
18. 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
19. TLSv1 must be negotiated with encryption and integrity.

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*