NSM Secure UI Crypto Module

Security Policy

Version: 1.4

Revision Date: April 1, 2010

CHANGE RECORD

Revision	***Date***	***Author***	***Description of Change***
1.0	11/13/2009	James Reardon	Initial Revision
1.1	11/23/2009	James Reardon	Added Algorithm Cert #'s
1.2	12/9/2009	James Reardon	Updated TBDs
1.3	12/10/2009	William Huan	Added Software Integrity Test
1.4	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 Secure UI Crypto Module provides cryptographic services for serving the Network Security Manager console by supporting a secure TLS session.

The McAfee NSM Secure UI Crypto Module is a software module designed to operate in compliance with FIPS 140-2 Level 2 security requirements.

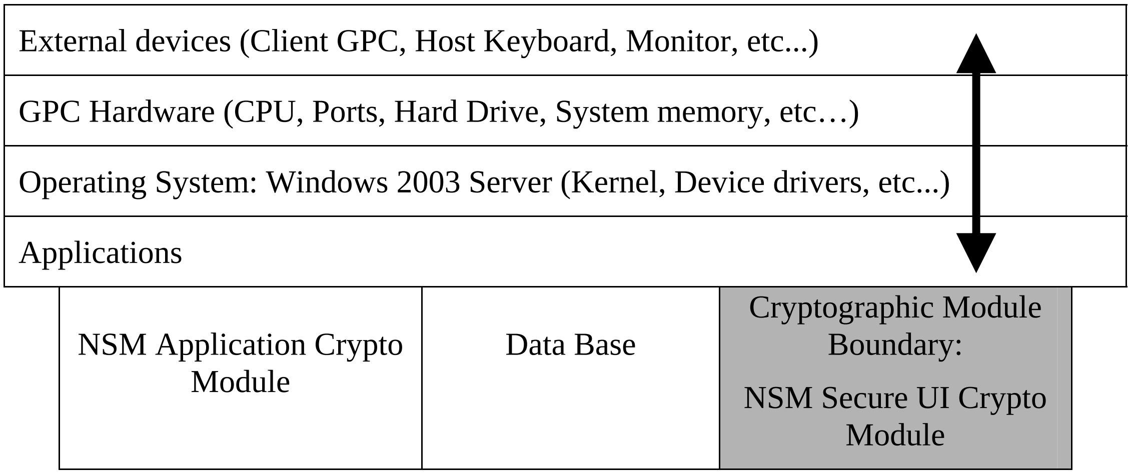
External devices (Client GPC, Host Keyboard, Monitor, etc...)
GPC Hardware (CPU, Ports, Hard Drive, System memory, etc…)
Operating System: Windows 2003 Server (Kernel, Device drivers, etc...)
Applications
NSM Application Crypto Module
Data Base
Cryptographic Module Boundary:
NSM Secure UI Crypto Module

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 Secure UI Crypto Module
Software Version: 1.0
Available in the following: McAfee NSM, 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. #
Open SSL TLSv1: AES 128 and 256-bit CBC mode	1238
Open SSL TLSv1: TDES 2 key/3key TCBC mode	886
Open SSL TLSv1: HMAC - SHA-1	722
Open SSL TLSv1: SHA-1	1136
Open SSL TLSv1: RSA Sign/Verify 1024, 2048	594
Open SSL TLSv1 and elsewhere: RNG ANSI X9.31	685
BSAFE: HMAC-SHA-1	721
BSAFE: SHA-1	1135

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
OpenSSL TLSv1: RSA Encryption for key establishment, the key transport method provides 80 bits or 112 bits of security strength.
OpenSSL TLSv1: MD5 and HMAC-MD5 within the TLS protocol. Not to be used with cipher-suite
OpenSSL 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
OpenSSLTLSv1:DES, RC4
OpenSSLTLSv1: 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, SNMP, 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, TLS User, System User and Cryptographic Officer (CO).

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	Passwords are a minimum of 8 characters chose from a 96 character set. 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
System User	GPC/OS System User The User role may have access to all services provided to the CO. This will be determined by the privileges assigned by the CO to the User.	Passwords are a minimum of 8 characters chose from a 96 character set. 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
TLS User/ Client	The role establishes secure sessions transmit data to and receive data from the host system. The cryptographic module enforces the separation of roles using web-server session IDs.	The module supports RSA (1024 or 2048-bit) signature verification, which has a computable resistance to attack of either 2^80 or 2^112 depending on the modulus size. Thus, the probability of a successful random attempt is 1/(2^80) or 1/(2^112), which are both less that 1/1,000,000. Due to processing speed restraints, the amount of signature verifications performed in a one minute period cannot exceed 100,000. Therefore, the probability of successfully authenticating to the module within one minute is 100,000/ (2^80) or 100,000/ (2^112), which are both less than 1/100,000.	TLS – certificate validation. CAC-PKI – Client Certificate.

5 Access Control Policy

5.1 Roles and Services

Table 7 – Authenticated Services

CO	System User*	TLS User/client	Service	Description
X	X		GPC/OS System Administration services	Maintain System and OS And Ensure FIPS compliant configuration of the Operational environment. Zeroize (allocated to CO by policy – see Security Rule #12 in Section 7) Self-Tests
X	X		Security Admin Services, CAC configuration	Configure and manage module.
		X	Manage Session	Manage connection to host system with client via TLSv1.

(*) – The System 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.

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
NSM UI Web-Server Private Key	Supports TLSv1 with user browsers.	RSA 1024 or 2048
UI Session Keys - Confidentiality	TLS session derived keys for encryption /decryption. TDES or AES	AES 128, 256 bits TDES 2-key/3-key, 168 bits
UI Session Keys - Integrity	TLS session derived keys for integrity – MAC secrets	HMAC-SHA-1
UI Session Key – Shared Secret	TLS pre-master secret used to derive session keys	TLSv1 KDF
OpenSSL DRNG Seed/Seed Key	DRNG state for OpenSSL AES-128Key - AES-256Key	ANSI x9.31 RNG
NSM Shared Secret	Shared secret authentication data for NSM communication	Authentication
CO/User - 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
UI Client Connection Public Key	RSA 1024 or 2048	Used to authenticate the client via TLS.
CAC Trusted Certificate Authorities Public Keys	RSA 1024 or 2048	Used for Client authentication through browser
NSM UI Web-Server Public Key	RSA 1024 or 2048	Used within TLSv1 for key transport.

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
CO, System User	GPC/OS System Administration services	R, W, Z	All CSPs
CO, System User	Security Admin Services, UI web- server CAC configuration	E, W	NSM UI Web-Server Private Key
TLS User/Client	Manage Session	E, W, Z	UI Session Keys - Confidentiality
		E, W, Z	UI Session Keys - Integrity
		E, W, Z	UI Session Key – Shared Secret
		E, W	NSM UI Web-Server Private Key

6 Operational Environment

The operational environment requires the following configuration process:

1. The module supports the use of Windows 2003 Server Standard Edition SP 2, on a Dell PowerEdge SC1420, 3.6 GHz Intel Xeon Processor (1 CPU), 32-bit, 2GB RAM. 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.
5. Use only Web browsers/ Java plug-ins that support TLSv1 and configure as defined in browser guidance and only enable FIPS ciphers and TLSv1.
6. The session client shall authenticate to the module via TLSv1 using signed certificates.

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. *TDES Encrypt and Decrypt Known Answer Tests*
            c. *SHA-1 Known Answer Test*
            d. *HMAC-SHA-1 Known Answer Test*
            e. *RNG, ANSI x9.31 Known Answer Test*
            f. *RSA Sign/Verify Known Answer Test*
            g. *RSA Encrypt/Decrypt Known Answer Test*
            h. *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 – ANSI X9.31
5. The module does not generate asymmetric Key pairs, thus Pair-wise consistency tests are not supported.
6. 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.
7. The operator shall be capable of commanding the module to perform the power-up self-test by cycling power or resetting the module service.
8. Power-up self tests do not require any operator action.
9. Data output shall be inhibited during self-tests and error states.
10. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
11. The module ensures that the seed and seed key inputs to the Approved RNG are not equal.
12. 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.
13. The module does support concurrent operators.

14. The module does not support a maintenance interface or role.
15. The module does not support manual key entry.
16. The module requires an external input/output device for entry/output of data, control and status as follows:
    - A client system and internet browser e.g. IEv6 and above**.**
17. The module does not output intermediate key values.
18. The module shall not be caused to share CSPs between the Approved and Non-Approved mode of operation.

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*