McAfee, Inc.
Network Security Platform Sensor M-6050 and M-8000 (M-8000 P and M-8000S)

Security Policy

Version 3.0

July 15, 2009

TABLE OF CONTENTS

1 Module Overview

The Network Security Platform (NSP) Sensor M-6050 and M-8000 (M-8000 P and M-8000 S) (HW P/Ns M-6050 (IAP-M65K-ISA, IFO-M65K-ISA, IIP-M65K-ISA) V1.4 and M-8000 (IAP-M80K-ISA, IFO-M80K-ISA, IIP-M80K-ISA) V1.4; FW Version 4.1.11.26) consists of the following multi-chip standalone platforms/configurations: M-6050, M-8000 P, and M-8000 S (where M-8000 P and M-8000 S run together as the M-8000). They are all Intrusion Prevention Systems (IPS) and Intrusion Detection Systems (IDS) designed for network protection. Both will offer protection against zero-day, DoS/DDoS, encrypted and SYN Flood attacks, and real-time prevention of threats like spyware, malware, VoIP vulnerabilities, phishing, botnets, network worms, Trojans, and peer-to-peer applications. The M-6050 and M-8000 are essentially identical except the M-8000 (i.e., the M-8000 P and M-8000 S running together) has increased throughput. The cryptographic boundary of each platform is the outer perimeter of the enclosure (not including the power supplies and fan trays).

Figure 1 shows the module and its cryptographic boundary.

Figure 1 – Image of the Cryptographic Module

2 Security Level

The cryptographic module meets the overall requirements applicable to Level 2 security of FIPS 140-2. Table 1 specifies the levels met for specific FIPS 140-2 areas.

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	2
Operational Environment	N/A
Cryptographic Key Management	2
EMI/EMC	2
Self-Tests	2
Design Assurance	3
Mitigation of Other Attacks	N/A

3 Modes of Operation

The module supports both a FIPS Approved and non-FIPS Approved mode of operation. If the module is to switch between the FIPS Approved and non-FIPS Approved mode of operation, the module will zeroize all CSPs and reboot. The cryptographic module may be configured for FIPS mode via execution of the "fips mode enable" command on the Command Line Interface (CLI) and operating the device per the Security Rules in Section 8. The cryptographic module may be configured for non-FIPS mode via execution of the "fips mode disable" command on the CLI. The user can determine if the module is running in FIPS vs. non-FIPS mode by executing the "Show Status" service.

3.1 FIPS Approved Mode of Operation

In FIPS mode, the module supports the following FIPS Approved algorithms:

- AES CBC mode with 128 bits for encryption and decryption (Cert. #880)
- Triple-DES CBC mode with 2 and 3 keys for encryption and decryption (Cert. #781)
- RSA with 1024 and 2048 bit keys for signature generation/verification (Cert. #425)
- DSA with 1024 bit keys for key generation, signature generation/verification (Cert. #345)
- SHA-1 and SHA-256 for hashing (Cert. #871)
- ANSI X9.31 DRNG with 2-Key Triple-DES ECB (Cert. #505)
- XYSSL RSA with 2048 bit keys for signature verification (Cert. #486)
- XYSSL SHA-1 for hashing (Cert. #970)

In FIPS mode, the module supports the following FIPS allowed algorithms and protocols:

- RSA with 1024 bit keys for key wrap decryption only (of bulk channel encryption/decryption key) – key wrapping; key establishment methodology provides 80 bits of encryption strength
- NDRNG for seeding the ANSI X9.31 DRNG
- TLS v1.0 (with algorithm tested ciphers)
- SSH v2 (with algorithm tested ciphers)

3.2 Non-FIPS Approved Mode of Operation

In non-FIPS mode, the module supports the following non-FIPS Approved algorithms:

- Blowfish for encryption
- DES for encryption/decryption
- MD5
- TACACS

4 Ports and Interfaces

The cryptographic module provides the following physical ports and logical interfaces:

- 10-Gig Monitoring Ports (Qty. 8): Data Input/Output
- 1-GigE Monitoring Ports (Qty. 8): Data Input/Output
- GigE Management Port (Qty. 1): Control Input, Data Output, Status Output
- GigE Response Port (Qty. 1): Data Output
- RS232 Console/Aux Ports (Qty. 2): Control Input, Status Output
- Compact Flash (Qty. 1): Data Input
- Power Entry Module (Qty. 2): Power Input
- Fan Tray Connector (Qty. 3): Control Input, Status Output, Power Output
- RJ11 Control Port (Qty. 8): Data Input, Power Output
- LEDs: Status Output

In the case of the M-8000 module (i.e., M-8000 P and M-8000 S used together), the number of ports are doubled. The M-8000 P and M-8000 S are connected in the following way:

- The "GigE Response Port" of the M-8000 P is connected to the "GigE Management Port" of the M-8000 S.
- A cross-connection between the M-8000 P and M-8000 S uses one pair of "10-Gig Monitoring Ports" on each. These ports are termed as cross-connect ports.

The module supports the following communication channels:

- Alert/Control channel (TLS)
- Packet log channel (TLS)
- Command channel (SNMP, plaintext)
- Bulk transfer channel (All is encrypted output)
- Install channel: Only used to associate a Sensor with the ISM (i.e., NSP Manager, see Table 2). They use a "shared secret".

5 Identification and Authentication Policy

The cryptographic module shall support four distinct operator roles (Admin, NSP Manager, M-8000 P, and M-8000 S). The cryptographic module shall enforce the separation of roles using role-based operator authentication. Table 2 lists the supported operator roles along with their required identification and authentication techniques. Table 3 outlines each authentication mechanism and the associated strengths.

Table 2 - Roles and Required Identification and Authentication

Role Availability Per Module Configuration			Role	Type of Authentication	Authentication Data
M-6050	**M-8000 P**	**M-8000 S**			
X	X	X	Admin (User)	Role-based operator authentication	Username and Password
X	X		NSP Manager (Cryptographic Officer) ***Note*:** The Network Security Platform Manager (NSP Manager) is a machine that manages multiple Network Platform Security Sensors (i.e., the cryptographic modules described in this Security Policy). The NSP Manager is also referred to as the ISM (IntruShield Security Manager) which is its former name.	Role-based operator authentication	Digital Signature (TLS), SNMPv3 Shared Secret
		X	M-8000 P (Cryptographic Officer)	Role-based operator authentication	Username and Password
	X		M-8000 S	Role-based operator authentication	Username and Password

Table 3 – Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
Username and Password	The password is an alphanumeric string of a minimum of eight characters chosen from the set of 62 printable and human-readable characters. The probability that a random attempt will succeed or a false acceptance will occur is 1/62^8 which is less than 1/1,000,000. After three failed authentication attempts, the module will enforce a 1 minute delay prior to allowing retry. The probability of successfully authenticating to the module within one minute is also 3/62^8 which are less than 1/100,000.
Digital Signature	RSA 1024 and 2048-bit keys are used for the signing (in isolated McAfee laboratory) and verification (by sensor) of digital signatures. The probability that a random attempt will succeed or a false acceptance will occur is 1/2^1024 which is less than 1/1,000,000. The module can only perform a single digital signature verification per second. The probability of successfully authenticating to the module within one minute is 60/2^1024 which is less than 1/100,000.

6 Access Control Policy

6.1 Roles and Services

Table 4 lists each operator role and the services authorized for each role. Following Table 4, all unauthorized services are listed.

Table 4 – Services Authorized for Roles

Role				Authorized Services
Admin	NSP Manager	M-8000 P	M-8000 S	
X	X	X	X	**Show Status**: Provides the status of the module, usage statistics, log data, and alerts.
X	X			**Network Configuration**: Establish network settings for the module or set them back to default values.
X	X			**Administrative Configuration:** Other various services provided for admin, private, and support levels.
X	X	X		**Firmware Update**: Install an external firmware image through TFTP or compact flash.
X				**Install**: Configures module for use. This step includes establishing trust between the module and the associated management station.
X				**Change Passwords**: Allows the Admin to change their associated passwords and the M-8000 Password.
X				**Certificate Management**: Provides the Admin the ability to install and export certificates.
X				**Zeroize**: Destroys all plaintext secrets contained within the module.
	X	X		**Intrusion Detection Management**: Management of intrusion detection policies and configurations through SNMPv3 and TLS.

Unauthenticated Services:

The cryptographic module supports the following unauthenticated services:

- **Self-Tests**: This service executes the suite of self-tests required by FIPS 140-2.
- **Intrusion Prevention Services**: Offers protection against zero-day, DoS/DDoS, encrypted and SYN Flood attacks, and real-time prevention of threats like spyware, malware, VoIP vulnerabilities, phishing, botnets, network worms, Trojans, and peer-to-peer applications. *Note:* No crypto is performed during this service.

6.2 Definition of Critical Security Parameters (CSPs)

The following are CSPs contained in the module:

- **Administrator Passwords**: Used for authentication of the "admin" role through console and SSH login. Extended services are given to the "admin" role by using the "support" or "private" passwords.
- **M-8000 Password:** Used for authentication of M-8000 P to the M-8000 S and vice-versa (i.e., authentication of the M-8000 P or S role).
- **Initialization Secret (i.e., Shared Secret)**: The only human input-able key used for mutual authentication of the sensor and ISM during initialization.
- **Bulk Transfer Channel Session Key**: Used to encrypt data packages across the bulk transfer channel.
- **SSH Host Private Keys**: Used for authentication of sensor to remote terminal for CLI access.
- **TLS Private Key**: Used for authentication of the sensor to ISM.
- **Seed for RNG**: Created by NDRNG and used to seed the ANSI X9.31 DRNG.
- **Seed Key for RNG**: Triple DES key used in the ANSI X9.31 DRNG and created by the NDRNG.

6.3 Definition of Public Keys:

The following are the public keys contained in the module:

- **McAfee FW Verification Key**: Used to authenticate firmware images loaded into the module.
- **SSH Host Public Key**: Used to authenticate the sensor to the remote client during SSH.
- **SSH Remote Client Public Key**: Used to authenticate the remote client to the sensor during SSH.

- **TLS Sensor Public Key:** Used to authenticate the sensor to ISM during TLS connections.
- **TLS ISM Public Key**: Used to authenticate ISM to sensor during TLS connections.

6.4 Definition of CSPs Modes of Access

Table 5 defines the relationship between access to CSPs and the different module services. The types of access used in the table are Read (R), Write (W), and Zeroize (Z).

Table 5 - CSP Access Rights within Services

	Administrator Passwords	M-8000 Password	Initialization Secret	Bulk Transfer Channel Session Key	SSH Host Private Keys	TLS Private Key	Seed for RNG	Seed Key for RNG	McAfee FW Verification Key	SSH Host Public Key	SSH Remote Client Public Key	TLS Sensor Public Key	TLS ISM Public Key
Show Status			R		R	R				R	R	R	R
Network Configuration			R		R	R				R	R	R	R
Administrative Configuration			R		R	R				R	R	R	R
Firmware Update			R		R	R				R	R	R	R
Install					R					R	R		
Change Password	R W	R W			R					R	R		
Certificate Management					R				R W	R W	R W	R W	R W
Zeroize		Z	Z	Z	R Z	Z	Z	Z		R	R		
Intrusion Detection Management				R		R						R	R
Self Tests													
Intrusion Prevention Services													

7 Operational Environment

The FIPS 140-2 Area 6 Operational Environment requirements are not applicable because the device supports a limited operational environment.

8 Security Rules

The cryptographic module's design corresponds to the 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 2 module.

1. The cryptographic module shall provide four distinct operator roles: Admin, NSP Manager, M-8000 P, and M-8000 S.
2. The cryptographic module shall provide role-based authentication.
3. When the module has not been placed in a valid role, the operator shall not have access to any cryptographic services.
4. The cryptographic module shall perform the following tests:

   A. Power up Self-Tests:

      1. Cryptographic algorithm known answer tests:
         a. AES CBC 128 encryption/decryption Known Answer Tests
         b. Triple-DES CBC encryption/decryption Known Answer Tests
         c. RSA 1024 and 2048 Sign/Verify Known Answer Test
         d. DSA 1024 Sign/Verify Known Answer Test
         e. SHA-1 Known Answer Test
         f. SHA-256 Known Answer Test
         g. ANSI X9.31 DRNG Known Answer Test
         h. RSA 1024 Decrypt Known Answer Test
         i. XYSSL RSA 2048 Verify Known Answer Test
         j. XYSSL SHA-1 Known Answer Test
      2. Firmware Integrity Test: XYSSL RSA 2048 used
      3. Critical Functions Tests: N/A

   B. Conditional Self-Tests:

         a. ANSI X9.31 DRNG Continuous Test
         b. NDRNG Continuous Test
         c. RSA Sign/Verify Pairwise Consistency Test
         d. DSA Sign/Verify Pairwise Consistency Test

e. External Firmware Load Test – XYSSL RSA 2048 used

6. 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 power cycling.
7. Data output shall be inhibited during key generation, self-tests, zeroization, and error states.
8. Status information shall not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
9. The module shall only support five concurrent SSH operators.
10. If a non FIPS validated firmware version is loaded onto the module, then the module is no longer a FIPS validated module.
11. The use of Telnet shall be restricted to the initialization of the cryptographic module.
12. The use of the Compact Flash Port shall be restricted to loading McAfee signed firmware.

9 Physical Security Policy

9.1 Physical Security Mechanisms

The cryptographic module includes the following physical security mechanisms:

- Production-grade components
- Production-grade opaque enclosure with tamper evident seals

9.2 Operator Required Actions

The operator is required to periodically inspect tamper evident seals. Table 6 outlines the recommendations for inspecting/testing physical security mechanisms of the module. If evidence of tamper is found during the periodic inspection, the operator should zeroize the module and modify Administrator Passwords upon start up. The operator should contact McAfee for new tamper labels, if necessary.

Table 6 – Inspection/Testing of Physical Security Mechanisms

Physical Security Mechanisms	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Tamper Evident Seals	As specified per end user policy	Visually inspect the labels for tears, rips, dissolved adhesive, and other signs of malice.
Opaque Enclosure	As specified per end user policy	Visually inspect the enclosure for broken screws, bent casing, scratches, and other questionable markings.

Figure 2 depicts the tamper label locations on the cryptographic module.

Figure 2 – Tamper Label Placement

10 Mitigation of Other Attacks Policy

The module has not been designed to mitigate any specific attacks beyond the scope of FIPS 140-2 requirements.