FIPS 140-2 Security Policy

Infraguard Processor Module

Advantor Systems
12612 Challenger Pkwy, Suite 300
Orlando, FL 32826
USA

October 26, 2011

Revision 1.14

Table of Contents

FIPS 140-2 Security Policy

Infraguard Processor Module

1. Introduction

The Infraguard Processor Module (IPM) is a mult-chip embedded encryption module coated with an opaque, tamper evident material. The cryptographic boundary is the entire module. The IPM is a plug-in module that is intended to meet FIPS 140-2, Security level 2 requirements.

The IPM is used to provide secure communications for Advantor Systems' physical security systems, communicating over either LAN or telephone line.

The module may be incorporated into multiple products, such as alarm panels (i.e. Infraguard II) and alarm receiving equipment (i.e. IMI-NET).

The IMI-NET receives alarm and status event data from up to 32 Infraguard II alarm panels connected via dedicated or dial-up telephone lines. Serial (modem) communications are encrypted with the IPM's Codeload application. Unencrypted data from the panel or receiver application is passed to and from Codeload using 'named pipes'. The IPM also allows the connection with a firewall device, such as the Cisco 5510, via IPSec, to provide secure communications over LAN. The IPMs and the firewall use preshared keys for encryption. All keys are managed with the Cryptoadmin application, including the serial devices' preshared keys and the VPNC.conf configuration settings.

1.1. Purpose

This document covers the secure operation of the IPM including the initialization, roles, and responsibilities of operating the product in a secure, FIPS-compliant manner.

1.2. Glossary

Term/Acronym	Description
IPM	Infraguard Processor Module
CO	Cryptographic-officer or Crypto-officer
ID	Identification number
VPNC	VPN client for Cisco ASA 5505 and 5510 firewall devices

2. Ports and Interfaces

Below is a mapping of the physical ports of this module to the logical interfaces.

Logical Interface	Physical Port
Data Input	240 pin DIMM connector 3,4 Ethernet RX 173 Modem RX 203-210 (I/O data bus)
Data Output	240 pin DIMM connector 1,2 Ethernet TX 172 Modem TX 203-210 (I/O data bus)
Control Input	240 pin DIMM connector 141 RS-232 TX (admin) 142 RS-232 RX (admin)
Status Output	240 pin DIMM connector 7 Ethernet link 8 Ethernet speed 9 Ethernet active 60 status LED 61 status LED
Power Interface	240 pin DIMM connector GND 6,15,17,19,24,39,40,129,130,163,164 GND 166,168,170,76,77,101,102,196,198 GND 200,202,226,228,230,232 3.3 VDC 16,18,37,39,165,167,169,192,193 3.3 VDC 197,199,201,227,229,231 5 VDC 113,114 1.2 VDC 161

3. Roles, Services, and Authentication

The IPM provides two different roles and a set of services particular to each of the roles. The two roles are ‘crypto-officer’ and ‘user’. The IPM will authenticate a crypto-officer’s identity by verifying login name and password. All encryption keys, including preshared keys for devices, and the VPN client configuration settings, are managed by Crypto-officers. The ‘user’ role is not authenticated, and has no access to the IPM security relevant data items (SRDI). When the IPM is in the ‘operation mode’, or ‘encrypt / decrypt data state’, user data is supplied to the IPM for encryption / decryption.

3.1. Roles

User Role

Users of the IPM, to secure communications over an untrusted network or modem channel, are not authenticated by the IPM. Users have no access to, or control over, the IPM’s security functions or SRDIs. Users supply unencrypted data to the IPM over the trusted interface for secure communications over an untrusted interface. The users sole-service is to communicate with a remote IPM.

Crypto Officer Role

The Crypto-officer has access to the IPM’s administrative commands. A Crypto-officer must initialize a new IPM upon receipt and then can create a user, delete a user, or set a key for a specified panel number. Once authenticated, the Crypto-officer can perform any of the following services (commands):

- add user: login name (prompts for password, masks entry, confirms by duplicate entry)
- change password (prompts for key, masks entry, confirms by duplicate entry)
- delete user: login name
- unlock user (login name)
- set key: panel ID (prompts for key, masks entry, confirms by duplicate entry)
- network settings (server ip, DHCP, local ip, netmask, gateway)
- clear vpn configuration
- vpn configuration setting (prompts for entry, masks entry, confirms by duplicate entry)
- show network (displays network settings)
- show users (displays login names)
- show devices (device IDs that are assigned a key, and key size)
- show status
- maintenance
- selftest
- zeroize

Maintenance Role

The maintenance role is for updating or repairing the IPM module by the manufacturer. A Crypto-officer may command the module to enter maintenance mode (see above). When the module is placed in maintenance mode, it is zeroized and all IPM cryptographic functions are disabled, including the administration console. When the module is restarted from maintenance mode, the maintenance mode will automatically be cleared, the module will be zeroized, and the module will be rebooted for standard operation. As the maintenance role, an operator has access to the Zeroize, SSH Enabled and Update/Repair services.

3.2. Authentication Mechanisms and Strength

The IPM authenticates crypto-officers by login name and password. The IPM enforces password strength, requiring minimum 8 characters in length, at least one number, one symbol, one lower case character, and one upper case character. In all cases, password data entry is displayed with an asterisk "*" during entry, and no functions are provided to display passwords.

Login Authentication

Crypto-officers authenticate to the IPM using a login and password, a crypto-officer must log in to the Crypto-officer application using the RS-232 port. If the password is entered incorrectly 5 times, without a valid login, the login will be disabled until unlocked by another crypto-officer, or the module is zeroized.

Operation Mode

In the ‘operation mode’, user data is sent to, and received from, the IPM on the trusted interface (named pipes) and encrypted data is sent to, and received from, either another IPM, over a serial communications channel, such as a modem channel. or a network device, such as a firewall, using IPSec communications.

4. Secure Operation and Security Rules

In order to operate the Infraguard Processing Module securely, the operator should be aware of the security rules enforced by the module and should adhere to the physical security rules and secure operation rules required.

4.1. Security Rules

The security rules enforced by the IPM result from the security requirements of FIPS 140-2.

FIPS 140-2 Security Rules

The following are security rules that stem from the requirements of FIPS PUB 140-2. The module enforces these requirements when initialized into FIPS level 2 Mode.

1. When initialized to operate in FIPS level 2 Mode, the IPM only uses FIPS-approved or FIPS allowed cryptographic algorithms.
2. The IPM employs an ANSI X9.31 RNG.
3. The IPM provides authentication of operators by verifying the operator’s login name and password.
4. The IPM provides the Crypto-officer the capability the zeroize the plaintext critical security parameters contained within the IPM including the keys for serial communications and VPN network communications..
5. In no case will the IPM output any security relevant data items (SRDI), including device keys for serial communications, VPN keys for network communications, crypto officer passwords, etc.
6. Data entry for all SRDI keys and passwords is echoed with a mask * character.

4.2. Physical Security Rules

The owner of the IPM must periodically inspect the physical case of the IPM to ensure that no attacker has attempted to tamper the IPM. Signs of tampering include

- Deformation, scratches, or scrapes in the opaque, hard epoxy covering the Module.

4.3. *Secure Operation Initialization Rules*

The IPM provides the following approved algorithms:

Algorithms Supported	Modes/Mod sizes	Algorithm Certificate
AES ECB and CBC	128-bit, 256 bit	1736
HMAC	SHA1	1013
RNG	ANSI X9.31	924
SHS	SHA-1	1521

The IPM provides the following non-approved algorithms:

Algorithms Supported	Notes
Diffie-Hellman	Allowed in FIPS mode, provides between 80 and 112 bits of encryption strength; non-compliant less than 80-bits of encryption strength

Because FIPS 140-2 prohibits the use of non-FIPS approved algorithms while operating in a FIPS compliant manner, the Crypto-officer should adhere to the following rules to initialize a new IPM to ensure FIPS level 2-compliance:

1. Power-up the IPM
2. When the IPM enters the Uninitialized state, the operator should authenticate the IPM using the factory default login (administrator, advantor).
3. Before any crypto functions may be invoked, the operator must first change the default password [minimum 8 character password with at least one lower case character, upper case character, number and symbol].
4. After changing password, the operator should add additional crypto officer logins, as required, using the initialize the IPM using the ”add user” command. The operator should specify the following command parameters:
   - Login name
   - Login password: [minimum 8 character password with at least one lower case character, upper case character, number and symbol]
   - Note: Maximum login tries are set to 5. After lockout, another Crypto-officer must log in to clear.
   - Preshared key entry: device ID followed by key (device key entry is masked, and must be entered twice for confirmation)
   - VPNC parameters: IPSec Gateway, IPSec ID, IPSec Secret, DH group 2, 5 or 14 (all VPNC parameters are masked during entry, and must be entered twice for confirmation).
5. Authenticate as the newly created Crypto-officer by logging in with login name and password.
6. Create any additional login names and passwords for IPM operators. They can change their password after login.

When initialized in this fashion, the IPM will only use FIPS-approved algorithms and/or Diffie-Hellman, which is non-approved but allowed in FIPS mode. Note that any operator can determine the state of an IPM at any time by requesting the “show status” command, which will return the initialized state of the IPM as FIPS or FIPS_FAIL.

5. Definition of SRDIs Modes of Access

This section specifies the IPM's Security Relevant Data Items as well as the access control policy enforced by the IPM.

5.1. Cryptographic Keys, CSPs, and SRDIs

While operating in a level 2 FIPS-compliant manner, the IPM contains the following security relevant data items:

Key/CSP	Description	Generation/Entry	Storage / Zeroization
Firmware Integrity Key	A 32-byte key embedded within the IPM's firmware image. This key is used to verify the firmware integrity code attached to a new firmware image.	The value is part of the firmware image and not generated or entered.	The key is stored in the firmware image in plaintext in flash storage. The key is not zeroized.
Panel keys	Panel keys are used for encrypting and decrypting temporary 'session' keys. The panel keys are 128-bit or 256-bit AES pre-shared keys. A separate key is entered for each "panel ID". Up to 10,000 panel keys may be entered for the IMI-NET.	Panel keys are externally generated and entered via the serial interface by crypto-officer.	Panel keys are stored in plaintext in flash storage. Zeroization: The panel key store file is deleted during zeroization.
Session Keys	Session keys are 128-bit or 256-bit AES keys. After the temporary session key is created, it is AES encrypted using the panel key and transmitted to the connecting device.	The session key is generated by the approved RNG. The session key can be output in encrypted form using the panel key.	The session key is stored, in plain text, in volatile memory and is not persistent. The session keys are set to "0" when the module is zeroized.
VPNC configuration file	VPNC is an IPsec VPN client. VPNC is used by the IPM module for encrypting 'user application' communications traffic, over a TCP/IP network. VPN preshared keys are manually distributed.	The configuration file is manually distributed and entered into the module by the crypto-officer.	The configuration file is stored in plaintext within the flash storage in the vpnc.conf file. The vpnc.conf file is deleted when the module is zeroized.
Crypto-officer Login Passwords	Crypto-officer logins and passwords are stored in an 'admins' file, in Flash memory. This file has 'root only' access. The password is used for authenticating crypto-officer logins.	Passwords are entered manually by crypto officer, generated by means at the discretion of the crypto officer.	Passwords are stored in plaintext flash storage. The administrator login / password file "admins.txt" is deleted when the module is zeroized.

Key/CSP	Description	Generation/Entry	Storage / Zeroization
Diffie-Hellman Public/Private Primes	1024-2048-bit prime values used for key establishment as part of IKE	The values are generated using a prime generation method that uses the approved RNG.	The value is ephemerally stored in RAM and can be zeroized by power cycling the module.
RNG Seed	The value is used to initialize the approved X9.31 RNG.	The value is generated using the system entropy source.	The value is ephemerally stored in RAM and zeroized during power cycle.
RNG Seed Key	The value is used to initialize the approved X9.31 RNG.	The value is generated using the system entropy source.	The value is ephemerally stored in RAM and zeroized during power cycle.

5.2. Access Control Policy

The IPM allows controlled access to the SRDIs contained within it. The following table defines the access that an operator or application has to each SRDI while operating the IPM in a given role performing a specific operation. The permissions are categorized as a set of four separate permissions: read (r), write (w), execute (x), zeroize (z). If no permission is listed, then an operator outside the IPM has no access to the SRDI.

Advantor Infraguard Processing Module SRDI/Role/Service Access Policy		Panel Keys	Session Keys	Crypto-officer Passwords	VPNC configuration file	Firmware Integrity Key	Diffie-Hellman Public/Private Primes	RNG Seed	RNG Seed Key
Role									
User role									
Communicate with remote IPM		x	x				x	x	x
Crypto-officer Role									
CreateUser				w					
DeleteUser				w					
SetSerialKey		w							
SetIPSecGateway					rw				
SetIPSecID					rw				
SetIPSecSecret					rw				
Show users									
Show devices		r							
ChangePassword				w					
UnlockUser				w					
Selftest						x			
Zeroize		d	d	d	d			d	d
Maintenance role (manufacturer)									
SSH enabled									
Zeroize		d	d	d	d			d	d

6. Bypass Mode

This module contains a Bypass Mode.
Bypass mode is a user-level function that may only be invoked on an alarm receiving device (e.g. IMI-NET) if it is connected to a non-FIPS enabled IPM and no key exists for the remote device id, as identified in the initial connection communication, and the connecting device identifies itself using a protocol specified for 'bypass mode' communications.

7. Self-Tests

7.1. Power Up Self-Tests

This module contains the following Power Up Self-Tests

- AES KAT
- RNG KAT
- HMAC KAT
- Firmware Integrity Test

7.2. Conditional Self-Tests

The module contains the following conational self-tests

- Continuous Random Number Generation Test
- Bypass Test
- Firmware Load Test

8. Mitigation of Other Attacks

This section is not applicable

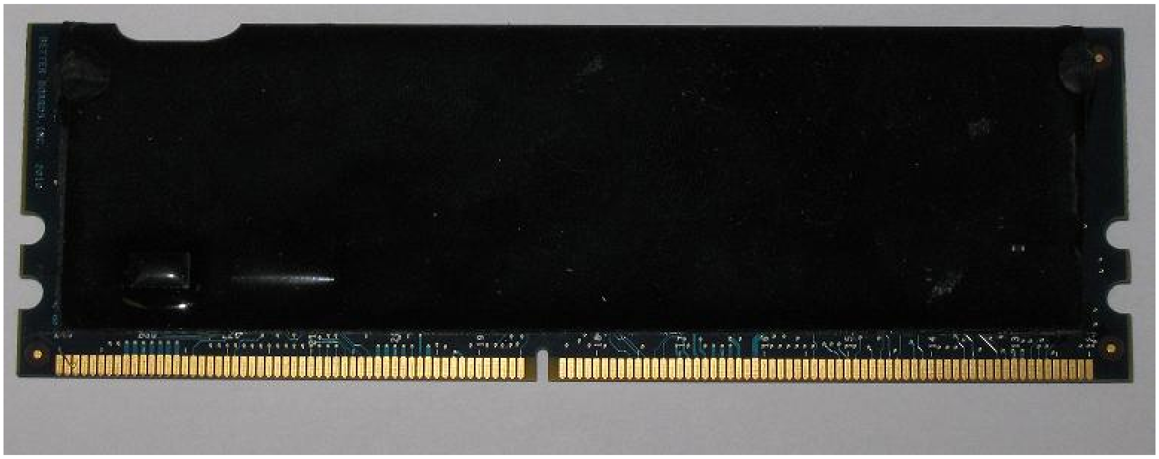
9. Cryptographic Boundary

The cryptographic boundary is the entire IPM module.

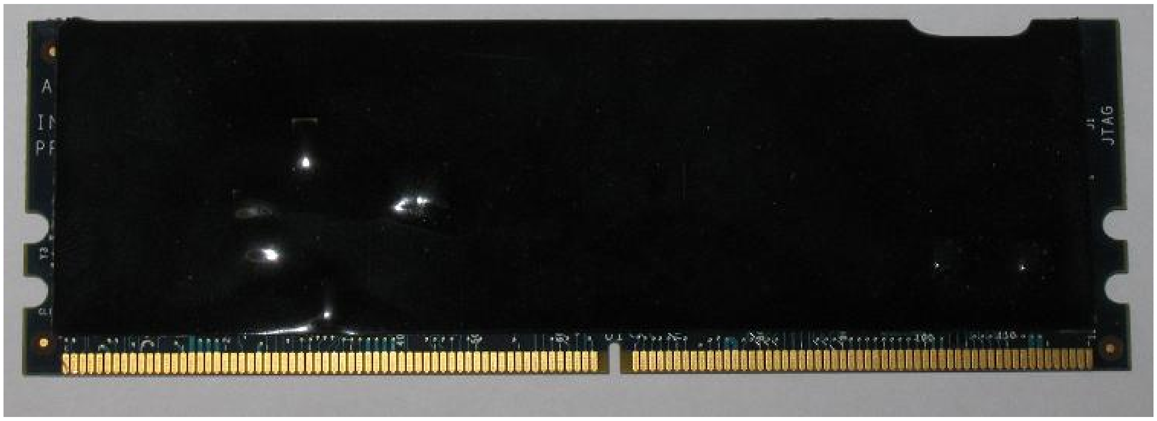
10. Revision Levels:

Hardware revision level: 5.1
Firmware: version 1.01

11. IPM Image - Front



12. IPM Image - Back



13. Secure Delivery

The security of the IPM cannot be assured if the device is received from the factory with evidence of tampering. If the shipping packaging of the product, or the tamper evident coating on the IPM show signs of tampering, contact an Advantor Systems customer service representative.