The Xirrus Wi-Fi Array
XS4, XS8
Security Policy

Document *Version 1.0*

Xirrus, Inc.

March 8, 2011

TABLE OF CONTENTS

1. MODULE OVERVIEW 3

2. SECURITY LEVEL 3

3. MODES OF OPERATION 4

4. IMPLEMENTING FIPS SECURITY 5

TO CHECK IF AN ARRAY IS IN FIPS MODE: 6
TO IMPLEMENT FIPS 140-2, LEVEL 2 USING CLI: 6

5. PORTS AND INTERFACES 7

6. IDENTIFICATION AND AUTHENTICATION POLICY 7

7. ACCESS CONTROL POLICY 8

ROLES AND SERVICES 8
DEFINITION OF CRITICAL SECURITY PARAMETERS (CSPS) 9

8. OPERATIONAL ENVIRONMENT 10

9. SECURITY RULES 10

10. PHYSICAL SECURITY POLICY 11

PHYSICAL SECURITY MECHANISMS 11
OPERATOR REQUIRED ACTIONS 12

11. MITIGATION OF OTHER ATTACKS POLICY 14

12. DEFINITIONS AND ACRONYMS 14

1. Module Overview

The Xirrus Wi-Fi Array- Models XS8 and XS4 are multi-chip standalone cryptographic modules. The primary purpose for this device is to provide data security for wireless Internet Protocol (IP) traffic.

Figure 3 – Image of the Xirrus Wi-Fi Array XS8 – Top View

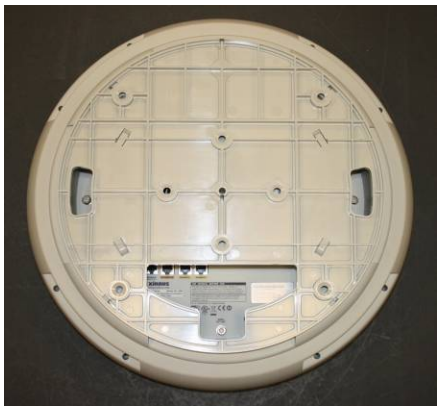


Figure 4 – Image of the Xirrus Wi-Fi Array XS8 – Bottom View

Figure 5 – Image of the Xirrus Wi-Fi Array XS4, Top View

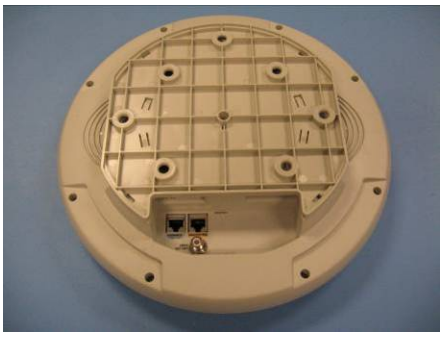


Figure 6 – Image of the Xirrus Wi-Fi Array XS4, Bottom View

The Xirrus Wi-Fi Arrays all use the same basic design. There are two form factors, a small one for 4 radio Arrays and a larger one for 8 radio arrays. The XS8 models use 8 radios and the XS4 models use 4 radios. The same firmware is used in all models.

Table 1 – Part Number Table

Model	Part Number	Version	Firmware
XS4	190-0092-002	D1	3.5
XS8	190-0091-005	A1	3.5

2. Security Level

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

Table 2 - 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	3
Self-Tests	2
Design Assurance	2
Mitigation of Other Attacks	N/A

3. Modes of Operation

Approved mode of operation

In FIPS mode, the cryptographic module only supports FIPS Approved algorithms as follows:

- AES (Cert. #470; ECB and CBC 128-bit; encryption)
- AES (Cert. #470; CCM mode)
- AES (Cert. #1503; CBC 128 and 256 bit)
- TDES (Cert. #1005)
- HMAC-SHA-1 (Cert. #861)
- SHA-1 (Cert. #1326)
- RSA (Cert. #716)
- RNG based on ANSI X9.31 Appendix A.2.4 using AES Algorithm (Cert. #801)

The module implements the following Non-Approved algorithms allowed for use in the FIPS Approved Mode of Operation:

- Non-Approved RNG (/dev/urandom)
- MD5 for TLS session key derivation
- RSA for key establishment (Key wrapping; Key establishment methodology provides 80 bits of encryption strength)
- Diffie-Hellman for SSH key establishment (Key agreement; key establishment methodology provides 80 bits or 112 bits of encryption strength)
- RC4 (considered plaintext)

Non-FIPS mode of operation

In non-FIPS mode, the cryptographic module provides non-FIPS Approved algorithms as follows:

- RC4 for encryption/decryption
- MD5
- Software RNG(/dev/urandom)

4. Implementing FIPS Security

Wi-Fi Arrays may be configured to satisfy the requirements for Level 2 of Federal Information Processing Standard (FIPS) Publication 140-2. The procedure in this section lists simple steps that must be followed exactly to implement FIPS 140-2, Level 2. The procedure includes physical actions, and parameters that must be set in Web Management Interface (WMI) windows in the Security section and in other sections.

1. Enable HTTPS using the CLI if it is not already enabled, using the following command:

   Xirrus_Wi-Fi_Array(config)# https on

   This allows the Web Management Interface to be used for the rest of this procedure. HTTPS is enabled on Arrays by default.

2. Select the Tools/CLI window. Type ‘management’ and <return>. Type ‘fips on’ and <return>.

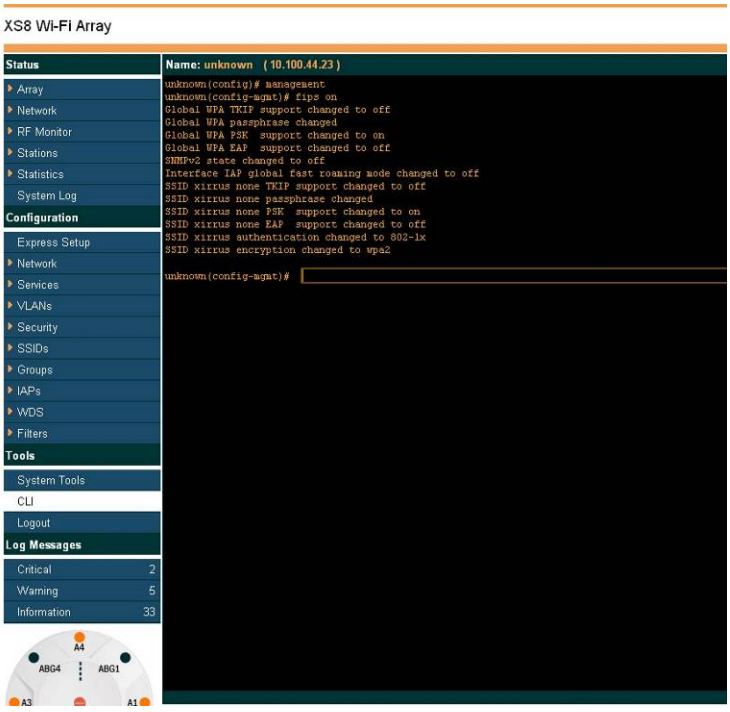


Figure 10 – SSID Management Window

To check if an Array is in FIPS mode:

You may determine whether or not the Array is running in FIPS mode by trying to change one of the security parameters shown in Figure 10. See example below:

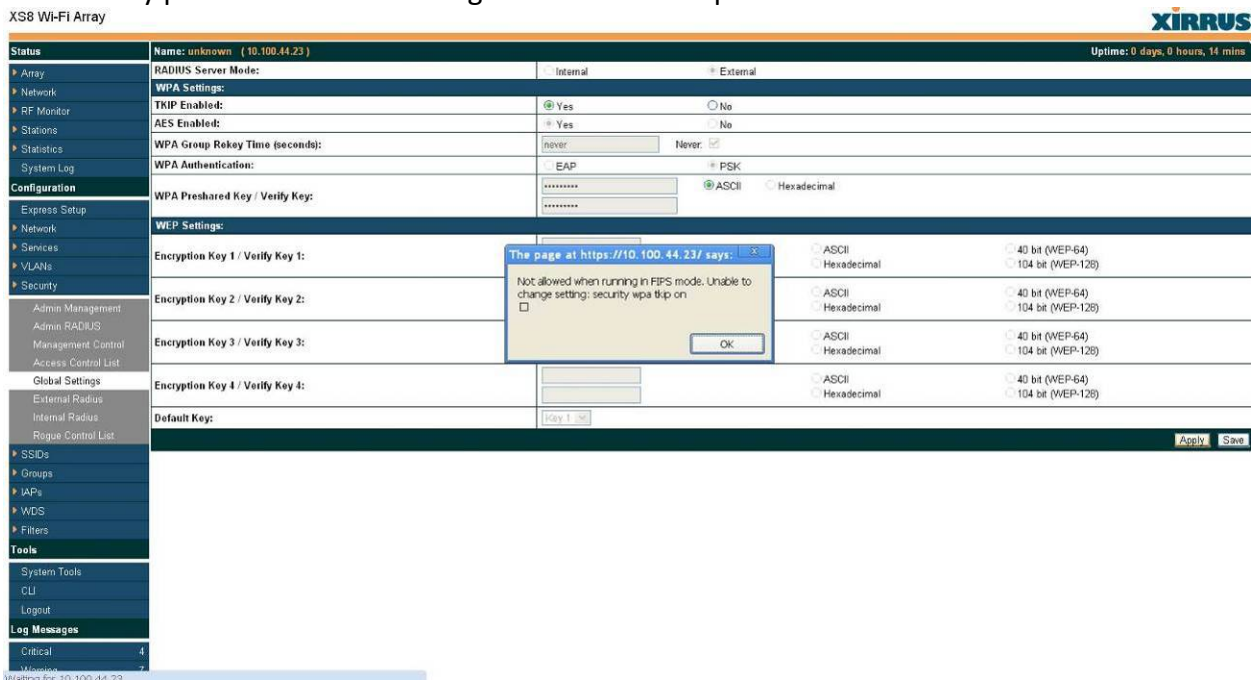


Figure 11 – Verify FIPs mode on

To implement FIPS 140-2, Level 2 using CLI:

1. The following CLI command will perform all of the settings required to put the Array in FIPS mode:

   Xirrus_Wi-Fi_Array(config)# fips on

   This command remembers your previous settings for FIPS-related attributes. They will be restored if you use the **fips off** command.

   Use the **save** command to save these changes to flash memory.

2. Use the **fips off** command if you would like to revert the FIPS settings back to the values they had before you entered the **fips on** command.

   Xirrus_Wi-Fi_Array(config)# fips off

   Use the **save** command to save these changes to flash memory.

5. Ports and Interfaces

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

Model	10/100 Ethernet Port	Gigabit Ethernet Port	Serial Port	TX/RX Radio Port	Status LEDs
XS4	N/A	1	1	4	6
XS8	1	2	1	8	12

- 10/100 Ethernet Port: data input, data output, control input, status output
- Gigabit Ethernet Port: data input, data output, control input, status output
- Serial Port (RS232): data input, data output, control input, status output
- TX/RX Radio Port: data input, data output
- LEDs: status output (Ethernet status, Integrated access point status, Array status)
- Power: POE

6. Identification and Authentication Policy

Assumption of roles

The cryptographic module shall support two distinct operator roles (User and Crypto Officer). The Crypto Officer role shall be performed by the Administrator managing the device, and the User role shall be performed by the wireless client using the device to send and receive data.

Table 3 - Roles and Required Identification and Authentication

Role	Type of Authentication	Authentication Data
Crypto Officer	Identity-based operator authentication	Username and Password
User	Role based operator authentication	Pre-Shared Key(PSK)

Table 4 – Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
Username and Password	Passwords are at least 5 characters long, with 94 characters available. Therefore, the probability that a random attempt will succeed or a false acceptance will occur is 1/7,339,040,224 which is less than 1/1,000,000. To exceed 1 in 100,000 probability of a successful random attempt during a 1-minute period, 73391 (1233 per second) attempts would have to be executed. This is not feasible from a standpoint of device capabilities.

Authentication Mechanism	Strength of Mechanism
PSK	802.11i Pre-Shared Key (PSK) is 32 bytes (256 bits) long, therefore there are 2^{256} possibilities for a PSK. This means that exceeding 1 in 100, 000 probability of a successful random attempt during a 1-minute period is not feasible from a device capabilities standpoint.

7. Access Control Policy

Roles and Services

Table 5 – Services Authorized for Roles

Role	Authorized Services
User: This role employs services to securely transport data over Wi-Fi.	• 802.11i with PSK: This service allows a user to authenticate and send/receive data in a secure manner using 802.11i PSK mode.
Crypto Officer (CO): This role manages the cryptographic module in a secure fashion over the CLI or WMI.	• Manage Configuration: This service allows an administrator to change the arrays configuration settings within the module such as establishing SSIDs, modifying usage of power, turning radios on/off, and adding new users. Additionally, it allows an administrator to perform the zeroization process, to load new firmware into the module and to display the module's current configuration and status.
Unauthenticated (UA): This role is assumed for services that do not require authentication to the module.	• Initiate Self-tests: This service executes the suite of self-tests required by FIPS 140-2. This is initiated by power cycling the array. • LED Status: Read available status output via LEDS.

Table 6 - Specification of Service Inputs & Outputs

Service	Control Input	Data Input	Data Output	Status Output
802.11i with PSK	Header info.	Data	Data	None
Manage Configuration	Instructions	Configuration Data	Configuration Data	Configuration Status
Initiate Self-Tests	Power	None	None	Success/fail
LED Status	None	None	None	Radio and array power and condition status

Definition of Critical Security Parameters (CSPs)

The following are CSPs contained in the module:

CSP	Description
Crypto Officer Password	This is an operator defined password (at least 5 characters long) that allows an administrator to log into the module. The password is stored on EEPROM as MD5 one-way hash. Destroyed after invocation of the zeroize service.
802.11i Pre-Shared Key (PSK) and Derived AES Session Key:	These are keys used for 802.11i encryption and integrity as well as User authenticatioin. The PSK is entered directly by operator via SSH or HTTPS and is stored on EEPROM in RC4 encrypted form (considered plaintext). Destroyed after invocation of the zeroize service.
TLS Session Keys	These are AES (128 or 256 bits) or TDES (128 bits) keys and HMAC-SHA-1 keys used to support HTTPS. These are derived from the Pre-Master Secret. Destroyed after invocation of the zeroize service.
TLS Pre-Master Secret	This Key is used to derive TLS Session keys. It is established by RSA transport during the TLS handshake. Immediately after invocation of the zeroize service.
TLS Private Key	RSA private key is used to decrypt TLS pre-Master Secret. Destroyed after invocation of the zeroize service.
SSH2 Session Keys	These are AES (128 or 256 bits) or TDES (128 bits) keys and HMAC-SHA-1 keys used to support SSH2 Sessions. These are derived from the SSH2 Shared Secret. Destroyed after invocation of the zeroize service.
SSH2 Shared Secret	This Key is used to derive SSH2 Session keys. It is established by Diffie-Hellman Key Agreement during the SSH2 negotiation. Destroyed after invocation of the zeroize service.
SSH2 Private Key	Ephemeral Diffie Hellman private keys used to establish the SSH2 Shared Secret. Destroyed after invocation of the zeroize service.
RNG State	Random number generator seed and seed key. Destroyed after invocation of the zeroize service.

Public Keys	Description
SSH2 Public Keys	Ephemeral Diffie-Hellman public keys used to establish the SSH2 Shared Secret
RSA Public key	Public key used to establish TLS session.

Table 7 – CSP Access Rights within Roles & Services

Roles			Service	Cryptographic Keys and CSPs Access
CO	User	UA		
	X		802.11i with PSK	Derive 802.11i AES Session Key using 802.11i PSK. Encrypt/decrypt data traffic using 802.11i AES Session Key.

X			Manage Configuration	Login using Crypto Officer's password Enter 802.11i PSK Enter/Change Crypto Officer password values. 'Zeroize' all plaintext CSPs. Use TLS Private Key, Pre-Master Secret and Session Keys Use SSH2 Private Key, Shared Secret and Session Keys
		X	Initiate Self-tests	None
		X	LED Status	None

8. Operational Environment

The FIPS 140-2 Area 6 Operational Environment requirements are not applicable because the Xirrus Access Point does not contain a modifiable operational environment.

9. Security Rules

The Xirrus Access Point's design corresponds to the cryptographic 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 two distinct operator roles. These are the User role and the Crypto Officer role.
2. The cryptographic module shall provide role-based and Identity-based authentication.
3. The module shall support concurrent operators.
4. The cryptographic module shall encrypt/decrypt data using the AES algorithm.
5. The cryptographic module shall perform the following tests:

   A. <u>Power up Self-Tests:</u>

      i. Cryptographic algorithm tests:
         - AES Known Answer Tests
         - TDES Known Answer Tests
         - RSA Known Answer Test
         - RNG Known Answer Test

      ii. Firmware Integrity Test (HMAC-SHA1)

   B. <u>Conditional Self-Tests:</u>

iii. Continuous tests for RNG and Non-Approved RNG.

iv. Firmware Load Test (HMAC-SHA1)

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.
7. All data output shall be inhibited during power-up self-tests 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 support the use of Approved and specifically Allowed algorithms in the Approved mode of operation.
10. The module shall not share CSPs between modes of operation. CSPs shall not be maintained when entering and exiting the FIPS Approved Mode of Operation.
11. The following shall not be supported in the FIPS Approved Mode of Operation

- Management over IAPs
- SNMP v1, v2 and v3
- SSH1
- SSL 2.0 and 3.0
- RADIUS (Internal and external)
- Telnet
- FTP, TFTP
- HTTP
- WEP
- WPA TKIP
- WPA EAP
- Entry of PSK as passphrase

12. The module shall be configured as defined in the Physical security section of this Security Policy. The tamper evident seals and security strap shall be installed for the module to operate in a FIPS Approved mode of operation.

10. Physical Security Policy

Physical Security Mechanisms

The multi-chip standalone cryptographic module includes the following physical security mechanisms:

- Production-grade components and production-grade opaque enclosure
- Tamper evident seals.

Table 8 – Inspection/Testing of Physical Security Mechanisms

Physical Security Mechanisms	Recommended Frequency of Inspection	Inspection Guidance Details
Tamper Evident Seals	1 months	Look for attempted removal of seals or tamper lock on the array and mounting plate.

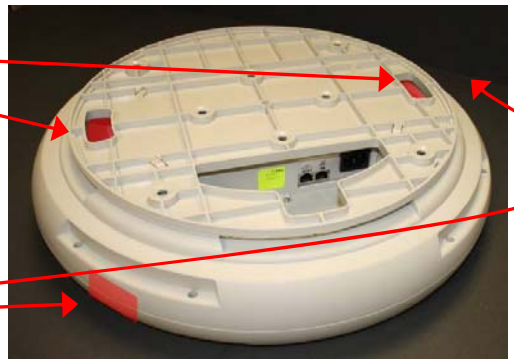
Operator Required Actions

The Cryptographic Officer is required to configure and periodically inspect the cryptographic module. Tamper evident seals and security straps shall be in control of the Cryptographic Officer at all times.

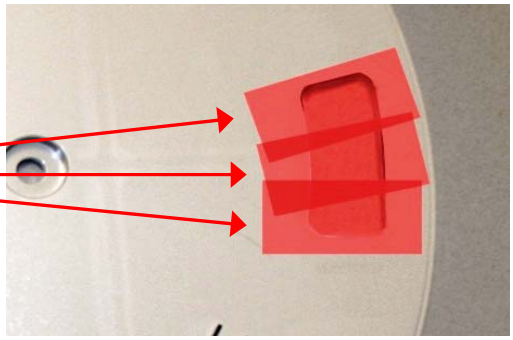
1. Apply two seals, one on either side of the Array about 180° apart from each other, as indicated in the figures below.
   - **IMPORTANT:**
     - **Before you apply the tamper-evident seal, clean the surface area of any grease, dirt, or oil. We recommend using alcohol-based cleaning pads for this. Each seal must be applied to straddle both sides of an opening so that it will show if an attempt has been made to open the Array.**
     - **Make sure that each seal straddles a seam.**

Tamper seal location covering mounting plate openings.

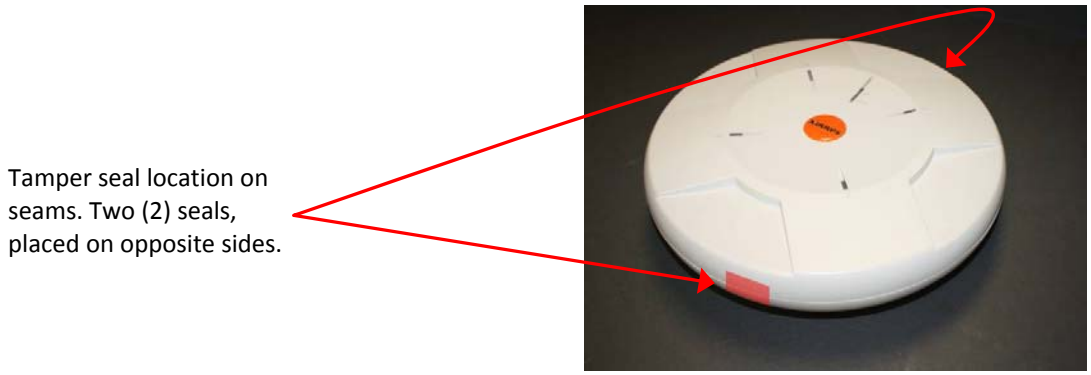
Tamper seal location on seams. Two (2) seals, placed on opposite sides.



Tamper seal location covering mounting plate openings. Six (6) seals placed, Three (3) across each opening. Place labels on mounting plate prior to mounting array body.



XS8 – Eight(8) total seals



XS4 – Two (2) total seals

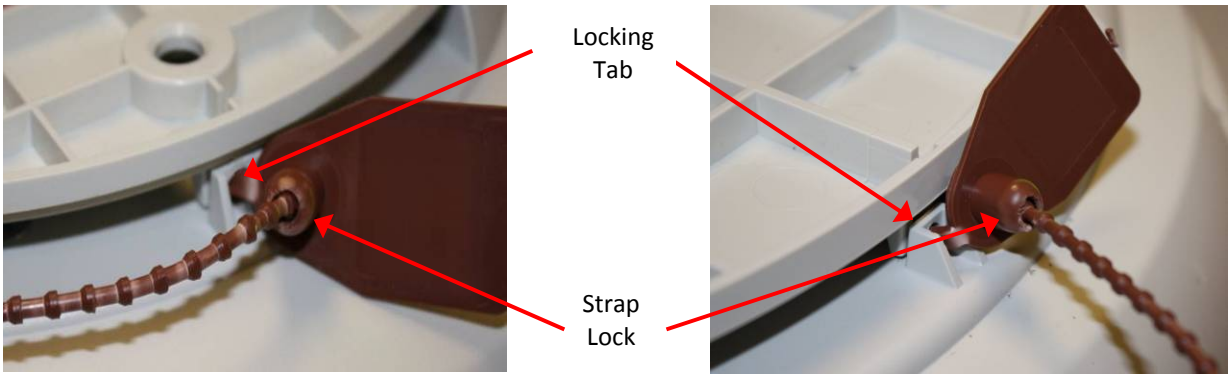
Figure 7 – Tamper-evident seal locations.
Location indicated by arrows and colored blocks

XS4 and XS8 - seam location

XS8 Mounting plate openings

Figure 8 – Tamper-evident seal appearance

2. Apply the supplied tamper-evident security strap to the unit as indicated in the figure below. Each mounting plate and array body contains a single locking tab. The Array body is mounted to the mounting plate and rotated until the mounting plate clicks into place and the locking tabs are aligned. The security strap is threaded through the aligned locking tabs and then pulled through the strap lock until firmly affixed. The security strap should be pulled tight to disallow turning of the mounting plate. Tamper evidence may be indicated by a broken strap or cracked locking tab.



XS4 **XS8**

Figure 9 – Apply the security strap as shown through locking tab

11. Mitigation of Other Attacks Policy

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

Table 9 – Mitigation of Other Attacks

Other Attacks	Mitigation Mechanism	Specific Limitations
N/A	N/A	N/A

12. Definitions and Acronyms

AES	Advanced Encryption Standard
CBC	Cipher Block Chaining
CCM	Counter with CBC-MAC
CRC	Cyclic Redundancy Check
ECB	Electronic Code-Book
FIPS	Federal Information Processing Standards
HMAC	Hash-based Message Authentication Code
HTTP	Hypertext Transfer Protocol
IAP	Integrated Access Points
LED	Light Emitting Diode
MAC	Message Authentication Code
MD5	Message-Digest #5
PSK	Pre-Shared Key
RADIUS	Remote Authentication Dial In User Service
RC4	ARCFOUR
RNG	Random Number Generator
SHA	Secure Hash Algorithm
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSL	Secure Sockets Layer
TDES	Triple – Data Encryption Standard
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security

TX/RX	Transmit / Receive
WEP	Wired Equivalent Privacy
Wi-Fi	IEEE 802.11 Wireless Networks
WMI	Web Management Interface
WPA	Wi-Fi Protected Access