MX-200R-GS/MX-216R-GS Mobility Exchange WLAN Controllers

Security Policy

Trapeze Networks

October 16, 2008

TABLE OF CONTENTS

1. Module Overview

The Trapeze Networks MX-200R-GS/MX-216R-GS Mobility Exchange WLAN Controllers (MX switches) HW P/Ns MX-200R-GS/MX-216R-GS Rev. A, FW Version MSS 6.1.0.3 and 6.1.0.4 are multi-chip standalone cryptographic modules, whose primary purpose is to provide secure wireless network communication. The diagram below illustrates the cryptographic boundary, which is defined as the outer perimeter of the enclosure. The power supplies (left sides) and power supply connectors are, for the purposes of FIPS 140-2, excluded from the cryptographic boundary.

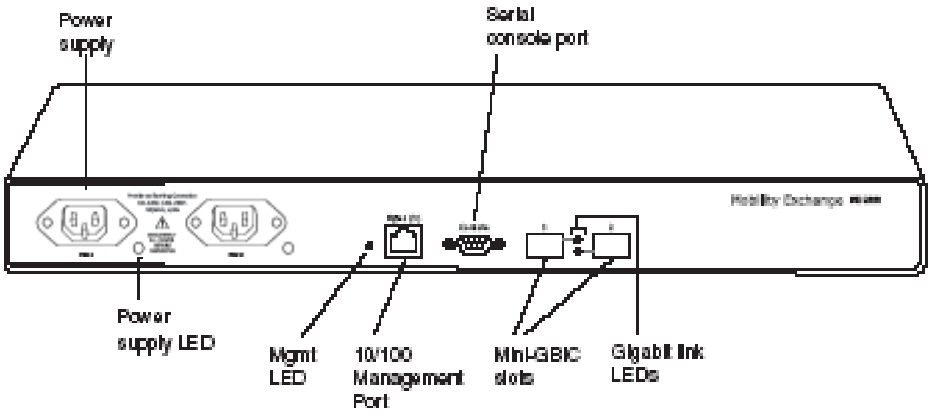

Figure 1 – MX-200R-GS Front Panel Control View

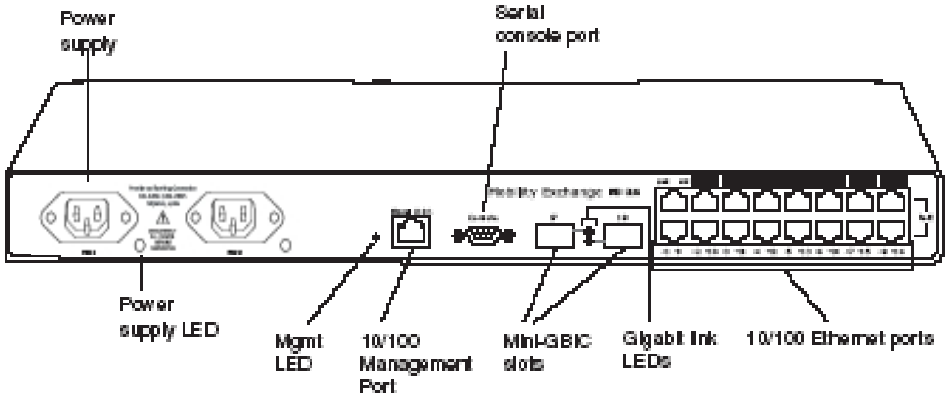

Figure 2 – MX-216R-GS Front Panel Control View

2. Security Level

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

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	2
Operational Environment	N/A
Cryptographic Key Management	2
EMI/EMC	2
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 supports FIPS Approved algorithms as follows:

- AES CCM (Cert. # 642)
- AES (Cert. #642)
- TDES (Cert. #594)
- SHA-1 (Cert. #677)
- HMAC SHA-1 (Cert. #331)
- RNG (Cert. #365)
- RSA Sign/Verify (Cert. #293)

The module also supports the following non-Approved algorithms:

- RSA Key Transport (key establishment; key wrapping with 1024 bit and 2048 bit keys has an effective strength of 80 bits and 112 bits respectively)
- DES (Not used to provide cryptographic strength)
- MD5 (Not used to provide cryptographic strength)
- NDRNG

The cryptographic module may be configured for FIPS mode via execution of "set FIPS-mode enable" through the System Configuration service. The user can determine if the cryptographic module is running in FIPS vs. non-FIPS mode via execution of the "Show System" service.

4. Ports and Interfaces

The cryptographic modules provide the following physical ports and logical interfaces:

- 10/100 Mbps Ethernet (Qty. 1): Control In, Data In/Out, Status Out
- Gigabit Ethernet (Qty. 2): Data In/Out, Status Out
- Serial Console (Qty. 1): Control In, Status Out
- LEDs: Status Out
- Power plugs (Qty. 2): Power In

The MX 216 provides the following additional ports:

- 10/100 Mbps Ethernet (Qty. 16): Control In, Data In/Out, Status Out, Power(PoE) out

5. Identification and Authentication Policy

Assumption of roles

The cryptographic module shall support three distinct operator roles (User, Cryptographic-Officer, and RADIUS Server). The User and CO authenticate through the use of alphanumeric passwords of eight (minimum) characters randomly chosen from the 95 printable and human-readable characters. The RADIUS Server authenticates to the module by means of proving knowledge of a shared secret. Upon power cycling the module, all previous authentications are cleared.

Table 2 – Roles and Required Identification and Authentication

Role	Type of Authentication	Authentication Data
User	Identity-based authentication	Username and Password
Cryptographic-Officer	Role-based authentication	Password
RADIUS Server	Role-based authentication	Knowledge of a shared secret (RADIUS Secret)

Table 3 – Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
Password (min length 8-characters)	The probability that a random attempt will succeed or a false acceptance will occur is 1/95^8 which is less than 1/1,000,000. The module restricts the number of failed authentication attempts to six. The probability of successfully authenticating to the module within one minute is also 6/95^8 which is less than 1/100,000.
Knowledge of a Shared Secret/Fingerprint verification	The shared secret is at least 16-bytes. The probability that a random attempt will succeed or a false acceptance will occur is at least 1/2^128 which is less than 1/1,000,000. The module will only allow a max of one attempt per minute. The probability of successfully authenticating to the module within one minute is also 1/2^128 which is less than 1/100,000.

6. Access Control Policy

Roles and Services

Table 4 – Services Authorized for Roles

Role	Authorized Services
User:	Show System Status – Display status and configuration information.
Cryptographic-Officer:	Show System Status – Display status and configuration information. System Configuration – Manage the general system and network settings. AAA Management – Configure the module's account settings, authentication parameters, and Access Control Lists (ACL). Key Management – Provides the facility to modify encryption settings, generate keys, and manage certificates. MP Access Point Management: Manage an attached MP Access Point.
Radius Server	Facilitate Authentication

Unauthenticated Services:

The cryptographic module supports the following unauthenticated services:

- Show Status: This service provides operational status of the cryptographic module through the LEDs.
- Self-Tests: This service executes the suite of self-tests required by FIPS 140-2.

Definition of Critical Security Parameters (CSPs)

The following are CSPs contained in the module:

Table 5 – CSP Descriptions

CSPs	Description
User password	Authenticates the User
Crypto officer (C.O.) password	Authenticates the C.O.
DRNG state	Used to generate random values for the ANSI X9.31 approved DRNG.
RADIUS secret	Authenticates the RADIUS server.
TLS session key	Provides data confidentiality for HTTPS traffic.
TLS HMAC integrity key	Provides data integrity for HTTPS.
TLS Pre-master secret	Used during TLS to establish session keys.
HTTPS TLS private key	Used during TLS to unwrap the pre-master secret; 1024-2048 bits in length.
EAP-TLS private key	Used during EAP-TLS to unwrap the pre-master secret; 1024 to 2048 bits in length.
MX secret	HMAC-SHA-1 key used to authenticate the MX to the Access Point (AP).
AP-MX Master Key	Used to provide data confidentiality using AES CCM 128. This key acts as the Master and Session Key.
MX-MX RSA Private key	Used during MX-MX key exchange to decrypt session key; key size is 2048 bits
MX-MX session key	Used for encrypting control traffic between MX and another MX through AES; key size is 256 bits
Software integrity key	Used to verify integrity of MX software image using HMAC-SHA1.
Pre-Shared Key (PSK)	Used as Pairwise Master Key for 802.11i; 32 bytes long
Master Key	Used to derive PMK for 802.1li
Pairwise Master Key (PMK)	Used to derive PTK for 802.11i; 32 bytes long
Pairwise Transient Key (PTK)	Used to derive KCK, KEK, and TK for 802.11i.
Key Confirmation Key (KCK)	Used as Key Integrity key; AES 128 bits
Key Encryption Key (KEK)	Used as Key encryption key to encrypt group key; AES 128 bits
Temporal Key	Used as data encryption key; AES 128 bits
Group Master Key (GMK)	Used to derive Group Transient Key; AES 128 bits
Group Transient Key (GTK)	Used for encrypting broadcast and multicast traffic; AES 128 bits

Definition of CSPs Modes of Access

Table 6 defines the relationship between access to CSPs and the different module services. The modes of access shown in the table are defined as follows:

- R - Read
- W- Write
- Z - Zeroize

Table 6 – CSP Access Rights within Roles & Services

CSPs\Services	Show System Status	System Configuration	AAA Management	Key Management	MP Access Point Management	Facilitate Authentication	Show Status	Self-Tests
User password	N/A	N/A	RWZ	N/A		R	N/A	N/A
Crypto officer (C.O.) password	N/A	N/A	RWZ	N/A		R	N/A	N/A
DRNG state	N/A	RW	N/A	RWZ		N/A	N/A	N/A
RADIUS secret	N/A	RW	RWZ			R	N/A	N/A
TLS session key	N/A	RW	N/A	RWZ		N/A	N/A	N/A
TLS HMAC integrity key	N/A	RW	N/A	RWZ		N/A	N/A	N/A
TLS Pre-master secret	N/A	RW	N/A	RWZ		N/A	N/A	N/A
HTTPS TLS private key	N/A	RW	N/A	Z		N/A	N/A	N/A
EAP-TLS private key	N/A	RW	N/A	Z		N/A	N/A	N/A
MX secret	N/A	W	N/A	Z		N/A	N/A	N/A
AP-MX Master Key	N/A	N/A	N/A	Z	RW	N/A	N/A	N/A
MX-MX RSA Private key	N/A		N/A	Z		N/A	N/A	N/A
MX-MX session key	N/A		N/A	Z		N/A	N/A	N/A
Software integrity key	N/A	N/A	N/A	N/A	N/A	N/A	N/A	R
Pre-Shared Key (PSK)	N/A		N/A	Z		N/A	N/A	N/A
Master Key	N/A		N/A	Z		N/A	N/A	N/A
Pairwise Master Key (PMK)	N/A		N/A	Z		N/A	N/A	N/A

Pairwise Transient Key (PTK)	N/A		N/A	Z		N/A	N/A	N/A
Key Confirmation Key (KCK)	N/A		N/A	Z		N/A	N/A	N/A
Key Encryption Key (KEK)	N/A		N/A	Z		N/A	N/A	N/A
Temporal Key	N/A		N/A	Z		N/A	N/A	N/A
Group Master Key (GMK)	N/A		N/A	Z		N/A	N/A	N/A
Group Transient Key (GTK)	N/A		N/A	Z		N/A	N/A	N/A

7. Operational Environment

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

8. Security Rules

The cryptographic module'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 three distinct operator roles. These are the User role, the Cryptographic-Officer role, and the RADIUS Server role.
2. The cryptographic module shall provide role-based authentication for the CO and RADIUS Server, but identity-based authentication for the User.
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:

   Power up Self-Tests:

   1. Cryptographic algorithm tests:

      - TDES Known Answer Test
      - AES Known Answer Tests
      - SHA-1 Known Answer Test (Tested as part of the HMAC SHA-1 KAT)
      - HMAC SHA-1 Known Answer Test
      - RSA Sign/Verify Known Answer Test (SW)

- RSA Encrypt/Decrypt Known Answer Test (SW & HW)
- DRNG Known Answer Test

2. Software Integrity Test (HMAC SHA-1 Verification)

3. Critical Functions Tests: N/A

Conditional Self-Tests:

1. Continuous Random Number Generator Test (DRNG and NDRNG)

2. RSA Pairwise Consistency Test (Sign/Verify and Encrypt/Decrypt)

5. Data output shall be logically disconnected or inhibited during key generation, self-tests, zeroization, and error states.
6. Status information shall not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
7. The cryptographic module does not support a bypass capability or a maintenance mode.

9. Physical Security Policy

Physical Security Mechanisms

The cryptographic modules include the following physical security mechanisms:

- Production-grade components and production-grade opaque enclosure with tamper evident seals.

Operator Required Actions

The operator is required to periodically inspect tamper evident seals and install in the locations dictated below.

Table 7 – Inspection/Testing of Physical Security Mechanisms

Physical Security Mechanisms	Inspection/Test Guidance Details
Tamper Evident Seals	Three tamper evident labels should be applied to the module. The placement is as follows: 1. Top-front (*Figure 3*) 2. Rear Left 3. Rear right rear *(Figure 4)* 4.

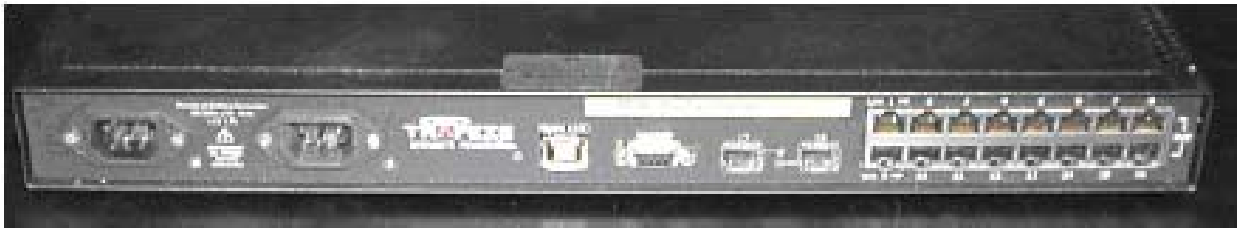

Figure 3 – MX-216R-GS Label Placement (Top-Front)

Figure 4 – Label Placement (Rear-Right)

10. Mitigation of Other Attacks Policy

Wireless Intrusion Detection and Protection

Trapeze has always built in core intrusion prevention capabilities as part of the Trapeze Mobility System, which includes detection of common WLAN attacks like address masquerading, RF jamming, weak WEP IV detection, and rogue detection and disablement. It also detects and alerts IT about denial of service (DoS) attacks, flood attacks, unauthorized SSIDs, deauthentication attacks, null probes, decryption errors and spoofed APs. It can also detect devices using wireless bridging and notify IT. In response to a detected attack, Trapeze Smart Mobile generates messages and SNMP traps and can perform countermeasures if policy dictates.

11. Definitions and Acronyms

- AAA Authentication, Authorization, Accounting
- ACL Access Control Lists
- AES CCM Advaced Encryption Standard
- AP Access Point
- CCM Counter with CBC-MAC
- DES Data Encryption Standard
- EAP Extensible Authentication Protocol
- GMK Group Master Key
- GTK Group Transient Key
- HMAC Keyed Hash Message Authentication Code
- IGMP Internet Group Management Protocol
- KCK Key Confirmation Key
- KEK Key Encryption Key
- MD5 Message Digest Algorithm 5
- NDRNG Non-Deterministic Random Number Generator
- PMK Pairwise Master Key
- PSK Pre-Shared Key
- PTK Pairwise Transient Key
- RADIUS Remote Authentication Dial In User Service
- RNG Random Number Generator
- RSA Rivest Shamir Adleman
- SHA Secure Hash Algorithm
- STP Spanning Tree Protocol
- TDES Triple Data Encryption Standard
- TLS Transport Layer Security
- VLAN Virtual Local Area Network