MP-422F Mobility Point

Security Policy

Trapeze Networks

August 14, 2009
# TABLE OF CONTENTS

1. MODULE OVERVIEW ............................................................................................................. 3

2. SECURITY LEVEL .................................................................................................................. 4

3. MODES OF OPERATION ......................................................................................................... 4

4. PORTS AND INTERFACES ...................................................................................................... 5

5. IDENTIFICATION AND AUTHENTICATION POLICY ........................................................... 5

6. ACCESS CONTROL POLICY ................................................................................................ 6

   ROLES AND SERVICES........................................................................................................ 6

   UNAUTHENTICATED SERVICES: ...................................................................................... 6

   DEFINITION OF CRITICAL SECURITY PARAMETERS (CSPs) ........................................ 6

   DEFINITION OF PUBLIC KEYS ......................................................................................... 6

   DEFINITION OF CSPs MODES OF ACCESS ................................................................. 7

7. OPERATIONAL ENVIRONMENT ............................................................................................ 8

8. SECURITY RULES ................................................................................................................... 8

9. PHYSICAL SECURITY POLICY ............................................................................................ 8

   PHYSICAL SECURITY MECHANISMS .............................................................................. 8

   OPERATOR REQUIRED ACTIONS ................................................................................ 8

10. MITIGATION OF OTHER ATTACKS POLICY ..................................................................... 9

11. DEFINITIONS AND ACRONYMS ....................................................................................... 10
1. Module Overview

The Trapeze Networks MP-422F Mobility Point (access point) HW P/N MP-422F Rev. A, FW Versions MSS 6.1.1.2.0, 6.1.0.3 and 6.1.0.4 is a multi-chip standalone cryptographic module, whose primary purpose is to provide secure network communication to and from wireless users and connect them to an MX switch. The cryptographic boundary is defined as being the outer perimeter of the enclosure; the diagram below illustrates the cryptographic boundary.

![Image of the Cryptographic Module (Top)](image)

**Figure 1 – Image of the Cryptographic Module (Top)**

![Image of the Cryptographic Module (Bottom)](image)

**Figure 2 – Image of the Cryptographic Module (Bottom)**
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

<table>
<thead>
<tr>
<th>Security Requirements Section</th>
<th>Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cryptographic Module Specification</td>
<td>2</td>
</tr>
<tr>
<td>Module Ports and Interfaces</td>
<td>2</td>
</tr>
<tr>
<td>Roles, Services and Authentication</td>
<td>2</td>
</tr>
<tr>
<td>Finite State Model</td>
<td>2</td>
</tr>
<tr>
<td>Physical Security</td>
<td>2</td>
</tr>
<tr>
<td>Operational Environment</td>
<td>N/A</td>
</tr>
<tr>
<td>Cryptographic Key Management</td>
<td>2</td>
</tr>
<tr>
<td>EMI/EMC</td>
<td>2</td>
</tr>
<tr>
<td>Self-Tests</td>
<td>2</td>
</tr>
<tr>
<td>Design Assurance</td>
<td>2</td>
</tr>
<tr>
<td>Mitigation of Other Attacks</td>
<td>N/A</td>
</tr>
</tbody>
</table>

3. Modes of Operation

Approved mode of operation

The cryptographic module only supports an Approved mode and supports the following Approved algorithms:

- AES CCM (Cert. #641)
- SHA-1 (Cert. #676)
- HMAC SHA-1 (Cert. #330)

The module also supports the following non-Approved algorithms:

- RSA Key Wrapping (1024-bit keys provide an effective strength of 80-bits)
- MD5
- RNG (non-compliant)
The Approved software may be determined by verifying the software version is the Approved version via execution of the “Show Version Details” service from an attached MX switch.

4. Ports and Interfaces

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

- 10/100 Mbps Ethernet (Qty. 2): Control In, Data In/Out, Status Out, Power In
- External RF Antenna (Qty. 2): Control In, Data In/Out, Status Out
- LEDs: Status Out

5. Identification and Authentication Policy

Assumption of roles

The cryptographic module shall support two distinct operator roles (User and Cryptographic-Officer).

<table>
<thead>
<tr>
<th>Role</th>
<th>Type of Authentication</th>
<th>Authentication Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>Role-based operator authentication</td>
<td>Knowledge of a Shared Secret (TK)</td>
</tr>
<tr>
<td>Cryptographic-Officer</td>
<td>Role-based operator authentication</td>
<td>Knowledge of a Shared Secret (MX Secret)</td>
</tr>
</tbody>
</table>

Table 3 – Strengths of Authentication Mechanisms

<table>
<thead>
<tr>
<th>Authentication Mechanism</th>
<th>Strength of Mechanism</th>
</tr>
</thead>
<tbody>
<tr>
<td>Knowledge of a Shared Secret</td>
<td>The shared secret is at least 32-bits and at most 256-bits in length. The probability that a random attempt will succeed or a false acceptance will occur is at least $1/2^{32}$ which is less than $1/1,000,000$. Network latency and processor performance prevent a brute force attack from being successful within a given minute. The probability of a random attempt successfully authenticating to the module within one minute is less than $1/100,000$ as a result of these resource restrictions.</td>
</tr>
</tbody>
</table>
6. Access Control Policy

Roles and Services

Table 4 – Services Authorized for Roles

<table>
<thead>
<tr>
<th>Role</th>
<th>Authorized Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>Secure Wireless Access: Allows the User to browse the network through an encrypted channel.</td>
</tr>
<tr>
<td>Cryptographic-Officer:</td>
<td>Establish Secure Session: Set-up an encrypted communication channel between the access point and the MX switch.</td>
</tr>
<tr>
<td></td>
<td>Configure: Specify the non-security relevant operational settings for the access point.</td>
</tr>
<tr>
<td></td>
<td>Monitor: Shows the status and statistics of the module.</td>
</tr>
<tr>
<td></td>
<td>Session Management: Install the User Transient Key or remove a User from the network.</td>
</tr>
<tr>
<td></td>
<td>Access Point Management: Reset/Zeroize the access point or Update the MX Secret.</td>
</tr>
</tbody>
</table>

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 and is invoked by power cycling the module.
- Show Status: Status information is available through the LEDs.

Definition of Critical Security Parameters (CSPs)

The following are CSPs contained in the module:

- MX Secret: Used to authenticate the CO to the module
- AP-MX Master Key: Used to encrypt traffic between the access point and MX
- AP-MX RSA Private Key: Used to unwrap the AP-MX Master Key
- Software Integrity Key: Used to verify the software integrity
- Transient Key: Used to provide data confidentiality for network traffic and authenticate the User.
- Group Transient Key: Used to provide data confidentiality for a network group

Definition of Public Keys
The following public key is contained in the module:

- **AP-MX RSA Public Key**: Used by an MX switch to wrap the AP-MX Master Key

### Definition of CSPs Modes of Access

Table 5 defines the relationship between access to CSPs and the different module services. The modes of access shown in the table are defined as follows:

- **Use**
- **Import**
- **Export**: N/A
- **Zeroize**

#### Table 5 – CSP Access Rights within Roles & Services

<table>
<thead>
<tr>
<th>Role</th>
<th>Service</th>
<th>Cryptographic Keys and CSPs Access Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>C.O. User</td>
<td>Secure Wireless Access</td>
<td>Use Transient Key or Group Transient Key</td>
</tr>
<tr>
<td>X</td>
<td>Establish Secure Session</td>
<td>Use MX Secret</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Import AP-MX Master Key</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Use AP-MX RSA Private Key</td>
</tr>
<tr>
<td>X</td>
<td>Configure</td>
<td>Use AP-MX Master Key</td>
</tr>
<tr>
<td>X</td>
<td>Monitor</td>
<td>Use AP-MX Master Key</td>
</tr>
<tr>
<td>X</td>
<td>Session Management</td>
<td>Use AP-MX Master Key</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Import Transient Key or Group Transient Key</td>
</tr>
<tr>
<td>X</td>
<td>Access Point Management</td>
<td>Use AP-MX Master Key</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Import MX-Secret</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Import AP-MX RSA Private Key</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Zeroize All CSPs</td>
</tr>
<tr>
<td>X</td>
<td>X</td>
<td>Show Status</td>
</tr>
<tr>
<td>X</td>
<td>X</td>
<td>Self-tests</td>
</tr>
</tbody>
</table>
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 two distinct operator roles. These are the User role, and the Cryptographic-Officer role.
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:
   
   Power up Self-Tests:
   1. Cryptographic algorithm tests:
      - AES CCM Known Answer Test
      - HMAC SHA-1 Known Answer Test
      - RSA Encrypt/Decrypt 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)
   2. Software Load Test (HMAC SHA-1 Verification)
   5. Data output shall be inhibited during 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.

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.

### Table 7 – Inspection/Testing of Physical Security Mechanisms

<table>
<thead>
<tr>
<th>Physical Security Mechanisms</th>
<th>Application Guidance Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tamper Evident Seals</td>
<td>The module includes two tamper labels, which should be applied on opposing sides, bridging the gap between the two halves of the enclosure.</td>
</tr>
<tr>
<td>Operators should periodically inspect tamper evident seals. If you should detect any evidence of tampering, you should inform your management and security office immediately.</td>
<td><strong>Upon placement of the seals, allow 24 hours for the adhesive seal to cure.</strong></td>
</tr>
</tbody>
</table>

*Each TEL’s position and corresponding serial no. should be recorded and logged for future reference.*

![Figure 3 – Tamper Label Placement](image)

### 10. Mitigation of Other Attacks Policy

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

- AES CCM  Advanced Encryption Standard Counter with CBC-MAC
- SHA   Secure Hash Algorithm
- MAC   Keyed Hash Message Authentication Code
- RNG   Random Number Generator
- RSA   Rivest Shamir Adleman
- MD5   Message Digest Algorithm 5
- DRNG  Deterministic Random Number Generator