Tropos Control Element Management System

Security Policy

Document *Version 3.3*

Tropos Networks

October 1st, 2009

TABLE OF CONTENTS

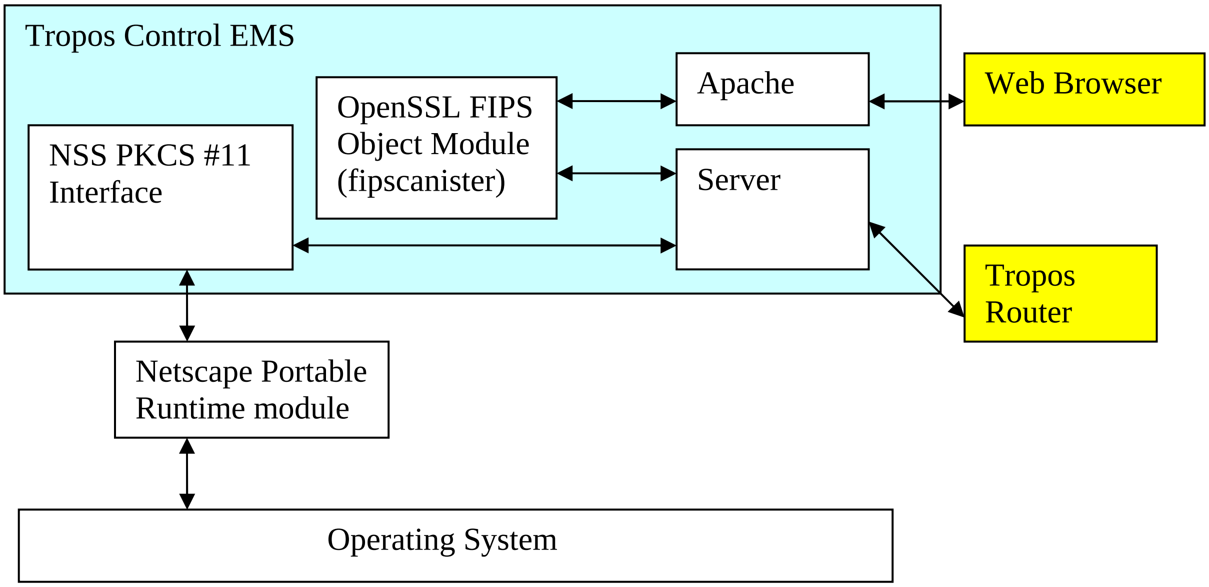
1. Module Overview

The Tropos Control Element Management System (EMS) device is a software only, multi-chip stand alone cryptographic module that runs on a general purpose PC computer. The primary purpose for this device is to monitor, configure Tropos Routers and control network traffic. The physical boundary of the module is the case of the PC.

The cryptographic module runs on all Linux operating environments though it is tested on CentOS 5 on 32-bit x86 platform. The software version of Tropos Control EMS is 7.3.

The logical cryptographic boundary of the Tropos Control EMS is shown in the Figure 1which consists of NSS PKCS #11 interface and Open SSL FIPS Object Module which is fipscanister.

Figure 1 – EMS Cryptographic Logical Boundary



2. Security Level

The cryptographic module meets the overall requirements applicable to Level 1 security of FIPS 140-2 and no components are excluded.

Table 2 - Module Security Level Specification

Security Requirements Section	Level
Cryptographic Module Specification	1
Module Ports and Interfaces	1
Roles, Services and Authentication	3
Finite State Model	1

Physical Security	N/A
Operational Environment	1
Cryptographic Key Management	1
EMI/EMC	1
Self-Tests	1
Design Assurance	1
Mitigation of Other Attacks	N/A

3. Secure Operation and Security Rules

In order to operate the Tropos Control 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.

Tropos Control has two modes of operation: non-FIPS Approved mode and FIPS Approved mode. By default the Tropos Control cryptographic module operates in the non-FIPS Approved mode. To operate the Tropos Control in FIPS Approved mode, CO has to change the FIPS mode from Administration tab-> Tropos Control Configuration in the Web Client.

FIPS Approved mode of operation

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

a) Tropos Control Cryptographic Library(OpenSSL)

- AES CBC
- RSA
- SHA-1
- HMAC SHA-1
- DRNG – X9.31 with AES (used by Apache while establishing connections with Browser based clients).
- Triple-DES CBC

b) Tropos Control Cryptographic Library (NSS) Algorithm Implementation

- AES ECB/CBC
- RSA
- SHA-1
- HMAC SHA-1
- DRNG -FIPS 186-2 (used for generation of TLS pre-shared master key for establishing TLS connection with the router)

- Triple-DES ECB/CBC

The module supports the following non-FIPS Approved algorithms and security functions that are allowed for use in FIPS mode:

- RSA (1024-bit) allowed in FIPS mode for key exchange used by TLS. This key establishment method provides 80-bits of security.

Non-FIPS mode of operation

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

- Blowcrypt for encryption
- MD5 for hashing

4. Ports and Interfaces

The Tropos Control provides the following physical and logical interfaces:

Table 2 – Physical and Logical interfaces

Physical Interface	Logical Interface	FIPS Defined Logical Interface
Network Port, Keyboard interface, Mouse interface	Web UI API parameters which accept data input to the module	Data input
Network Port, , PC Monitor, hard drive	Web UI API parameters which provide data output from the module	Data output
Power Port	N/A	Power Interface
Network Port, PC Monitor	Web UI API parameters which provide status output from the module	Status output
Network Port, PC Keyboard port, Mouse Port, PC Power button,	Web UI API which can be accessed by operators of the module	Control Input Interface

Table 3 – FIPS 140-2 Logical interfaces

FIPS Defined Logical Interface	Description
Data Input	The data input is: • All plaintext data entering Tropos Control application for purpose of being encrypted and stored. • All cipher text data entering Tropos Control application for the purpose of being decrypted.
Data Output	The data output is: • All plaintext data exiting the Tropos Control application • All cipher text data exiting the Tropos Control application
Control Input	The Tropos Control application accepts control input from the Operator. Control input consists of all commands and command parameters.
Status Output	The status output consists of all messages either logged by the module or returned by the module, and all status data obtained as a result of user commands.

5. Identification and Authentication Policy

Assumption of roles

The Tropos Control cryptographic module supports 3 distinct operator roles: Read Only User, Read Write User and Cryptographic Officer (CO). The Read Only user can monitor the network. The Read Write user can monitor and provision the network. CO can perform administration tasks like Router upgrade, User management including provisioning and monitoring.

Table 4 - Roles and Required Identification and Authentication

Role	Type of Authentication	Authentication Data
Cryptographic-Officer	Identity-Based operator authentication	Username and Password
Read/Write User	Identity-Based operator authentication	Username and Password
Read Only User	Identity-Based operator authentication	Username and Password

Table 5 – Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
Username and Password	All passwords must be a minimum of 8 characters chosen from a 72 character set. The probability that a random attempt will succeed or a false acceptance will occur is 1/72^8 which is less than 1/1,000,000. Due to processing speed constraints, the amount of password attempts per minute cannot exceed 100,000. Therefore, the probability of successfully authenticating to the module within one minute is 100,000/72^8 which is less than 1/100,000.

6. Access Control Policy

Roles and Services

Table 6 – Services Authorized for Roles

Role	Authorized Services
Cryptographic Officer	• Manage Network • Add or Delete Users • Upgrade EMS Software • Upgrade Router Software • Monitor Network Traffic (Show Status) • Monitor Network Reachability • Modify Router Configuration • FIPS Mode Enable/Disable • Self-Test • Modify EMS Configuration • Zeroization • Key Management

	• Add/Sync Routers
Read/Write User	• Modify Router Configuration • Monitor Network Traffic (Show Status) • Monitor Network Reachability • Add/Sync Routers
Read Only User	• Monitor Network Traffic (Show Status) • Monitor Network Reachability

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 by power cycling the module.

Definition of Critical Security Parameters (CSPs)

The following are CSPs contained in the module:

- Router-EMS Authentication Key
- Router Configurator Admin Password
- Router RADIUS Authentication Shared Secret
- Router RADIUS Accounting Shared Secret
- IPsec ISAKMP Shared Secret
- 802.11i Pre-Shared Key
- TLS Master Secret
- TLS Session Keys
- TLS (HTTPS) RSA Private Key
- Deterministic random number generator (DRNG) Seed
- Deterministic random number generator (DRNG) Seed Key
- NSS deterministic random number generator (DRNG) Seed Key
- EMS User Password

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:

Table 7 – CSP Access Rights within Roles & Services

Roles				
CO	**R/W User**	**Read Only User**	***Services***	**Cryptographic Keys and CSPs Access Operation**
X			Manage Network	All TLS Keys and Router-EMS Authentication Key
X			Add or Delete Users	EMS User Password
X			Upgrade EMS Software	N/A
X			Upgrade Router Software	Router Configurator Admin Password
X	X	X	Monitor Network Traffic (show Status)	EMS User Password
X	X	X	Monitor Network Reachability	EMS User Password
X	X		Modify Router Configuration	TLS Keys, Router-EMS Authentication Key, RADIUS Authentication shared secret, RADIUS Accounting shared secret, IPsec ISAKMP shared secret, DRNG Keys, 802.11i Pre-shared key
X			Modify EMS Configuration	EMS User Password
X			Zeroization	Destroy all unprotected Keys and CSPs
X			Key Management	Generating, modifying, and entering pre-configured keys (passwords, keys entered during manufacturing)
X	X		Add/Sync Routers	Router-EMS Authentication Key, DRNG Keys

7. Operational Environment

The FIPS 140-2 Area 6 Operational Environment requirements are applicable because the Tropos Control operates in a modifiable operational environment.

Tropos Control should be operated in a single user mode. Only one user account should be created in the OS.

Following steps should be performed to make the CentOS run in Single User Mode:

a. Log in as the "root" user.
b. Edit the system files `/etc/passwd` and `/etc/shadow` and remove all the users except "root" and the pseudo-users. Make sure the password fields in `/etc/shadow` for the pseudo-users are either a star (*) or double exclamation mark (!!). This prevents login as the pseudo-users.
c. Edit the system file `/etc/nsswitch.conf` and make `files` the only option for `passwd`, `shadow`, and `group`. This disables NIS and other name services for users and groups.
d. In the `/etc/xinetd.d` directory, edit the files `eklogin`, `gssftp`, `klogin`, `krb5-telnet`, `kshell`, `rexec`, `rlogin`, `rsh`, `rsync`, `telnet`, and `tftp`, and set the value of `disable` to `yes`.
e. Reboot the system for the changes to take effect.

8. Security Rules

This section documents the security rules enforced by the cryptographic module to implement the security requirements of Tropos Control.

1. The cryptographic module shall provide at least two distinct operator roles (User and CO roles). These are the Read Only User role, Read Write User role, and the Cryptographic-Officer role.

2. The cryptographic module shall provide identity-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 encrypt message traffic using the AES algorithm.

5. The cryptographic module shall perform the following tests:

   A. Power up Self-Tests:

   1. Cryptographic algorithm tests:

      a. AES Known Answer Test for OpenSSL

      b. AES Known Answer Test for NSS

      c. DRNG Known Answer Test for OpenSSL

d. DRNG Known Answer Test for NSS

e. SHA-1 Known Answer Test for OpenSSL

f. SHA-1 Known Answer Test for NSS

g. RSA Known Answer Test for OpenSSL

h. RSA Known Answer Test for NSS

i. HMAC Known Answer Test for OpenSSL

j. HMAC Known Answer Test for NSS

k. Triple DES Known Answer Test for OpenSSL

l. Triple DES Known Answer Test for NSS

2. Software Integrity Test (RSA signature verification)

B. Conditional Self-Tests:

1. Continuous Random Number Generator (CRNG) test – performed on NDRNG and DRNG for both OpenSSL and NSS

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. Prior to each use, the internal DRNG shall be tested using the conditional test specified in FIPS 140-2 §4.9.2.

8. Data output shall be inhibited during key generation, self-tests, zeroization, and error states.

9. Status information shall not contain CSPs or sensitive data that if misused could lead to a compromise of the module.

10. Configuration in FIPS Mode:

During initialization, the CO must perform the following configuration steps in order to be in FIPS mode:

a. Enable “FIPS Mode”

b. SSH access must be kept disabled

c. Set “Router-EMS Authentication Key”

d. “Password of all the EMS Operators must have minimum of 8 characters

e. EMS Database Password must have minimum of 8 characters.

f. Only Local authentication should be used and not Radius Authentication for Tropos Control users.

9. Physical Security Policy

The FIPS 140-2 Area 5 Physical Security requirements are not applicable because the Tropos Control is software only module.

10. Mitigation of Other Attacks Policy

The module has not been designed to mitigate any specific attacks.