FIPS 140-2 Security Policy
MRV LX-4000T Series

MRV Communications
295 Foster St.
Littleton, MA 01460
USA

December 4, 2008

Revision Version .34

FIPS 140-2 Security Policy

LX-4000T Series

1. Introduction

The following describes the security policy for the LX-4000T Series Console Servers. The LX Series is a key component of MRV's Out-of-Band Network solution. Out-of-Band Networks provide secure remote service port access and remote power control to devices in an organization's networks and infrastructures. This nearly eliminates the need for physical presence at a device to correct problems or manage its everyday operation. MRV's Out-of-Band Network solution includes console servers, terminal servers, device servers, remote power control and management system. These capabilities combined with FIPS 140-2 security make the LX Series an ideal choice for providing secure remote access in a variety of environments.

1.1. Purpose

This document covers the secure operation of the LX-4000T Series including initialization, roles, and responsibilities of operating the product in a secure, FIPS 140-2 compliant manner. Guidance provided in the security policy references procedures that can be found in the following references:

- Getting Started With The LX-4000T Series, 4510340f.pdf
- LX-4000T Quick Start Guide, 4510339G.pdf
- LX-Series Commands Reference Guide, Versions 5.3.0 and 5.3.0.1, 4510310ac.pdf.
- LX-Series Configuration Guide, Version 5.3.1, 4510364a.pdf
- Installing the LX-4000T Series, 4510342h.pdf

1.2. Versions

The module consists of two firmware images, linuxito and ppciboot, that have following firmware versions.

linuxito version : 5.3.1
ppciboot version: 5.3.1

For the LX-4000T Series there are twenty-four hardware configurations as described in Section 2.1. Therefore, there are
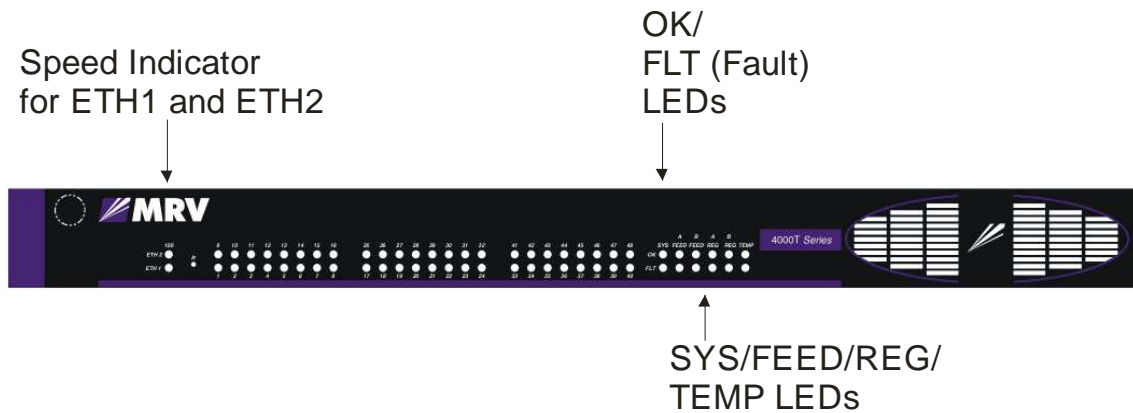
twenty-four hardware versions in the table below (hardware versions: 600-R3265 RevB through 600-R3288 RevB (inclusive)).

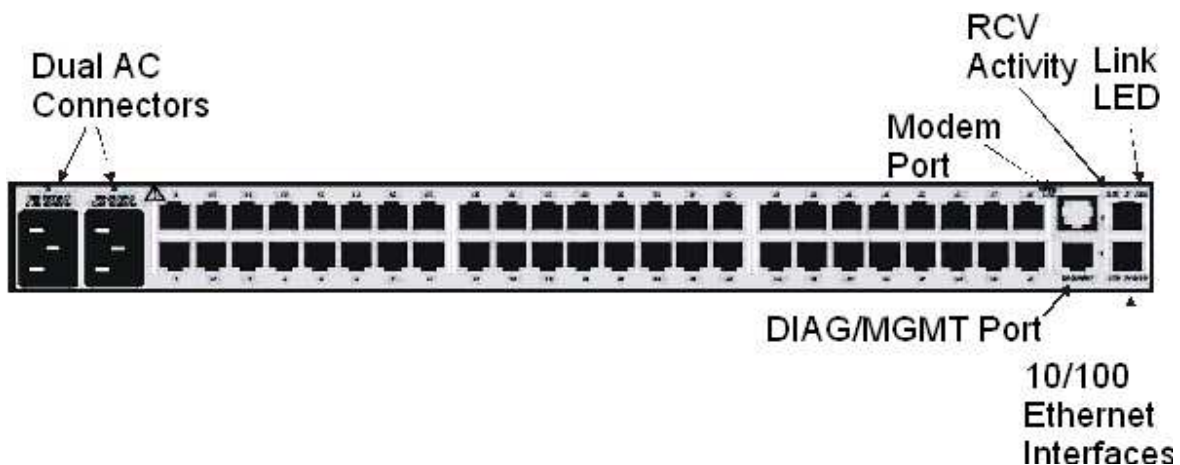| Model	Top Level	Rev	B/L	Rev
LX-4008T-001ACF	600-R3265	B	400-R0029	B
LX-4008T-002ACF	600-R3266	B	400-R0029	B
LX-4008T-012DCF	600-R3267	B	400-R0030	B
LX-4008T-101ACF	600-R3268	B	400-R0029	B
LX-4008T-102ACF	600-R3269	B	400-R0029	B
LX-4008T-112DCF	600-R3270	B	400-R0030	B
LX-4016T-001ACF	600-R3271	B	400-R0031	B
LX-4016T-002ACF	600-R3272	B	400-R0031	B
LX-4016T-012DCF	600-R3273	B	400-R0032	B
LX-4016T-101ACF	600-R3274	B	400-R0031	B
LX-4016T-102ACF	600-R3275	B	400-R0031	B
LX-4016T-112DCF	600-R3276	B	400-R0032	B
LX-4032T-001ACF	600-R3277	B	400-R0033	B
LX-4032T-002ACF	600-R3278	B	400-R0033	B
LX-4032T-012DCF	600-R3279	B	400-R0034	B
LX-4032T-101ACF	600-R3280	B	400-R0033	B
LX-4032T-102ACF	600-R3281	B	400-R0033	B
LX-4032T-112DCF	600-R3282	B	400-R0034	B
LX-4048T-001ACF	600-R3283	B	400-R0027	B
LX-4048T-002ACF	600-R3284	B	400-R0027	B
LX-4048T-012DCF	600-R3285	B	400-R0028	B
LX-4048T-101ACF	600-R3286	B	400-R0027	B
LX-4048T-102ACF	600-R3287	B	400-R0027	B
LX-4048T-112DCF	600-R3288	B	400-R0028	B

2. Interfaces

The LX-4000T Series are considered a multi-chip standalone module, and the cryptographic boundary of the module is defined by the outer case of module.

2.1. LX-4000T Series

Speed Indicator for ETH1 and ETH2

OK/ FLT (Fault) LEDs

SYS/FEED/REG/ TEMP LEDs

Dual AC 4048T Front Panel

Dual AC Connectors

RCV Activity Link LED

Modem Port

DIAG/MGMT Port

10/100 Ethernet Interfaces

Dual AC 4048T Rear Panel

- **LX-4008T-001ACF LX-4000T** with (8) RS232 RJ45 ports, & single AC power

- **LX-4008T-002ACF LX-4000T** with (8) RS232 RJ45 ports, & dual AC power

- **LX-4008T-012DCF LX-4000T** with (8) RS232 RJ45 ports, & dual DC (36-72V) power

- **LX-4008T-101ACF LX-4000T** with (8) RS232 RJ45 ports, & single AC power & internal V.90 modem

- **LX-4008T-102ACF LX-4000T** with (8) RS232 RJ45 ports, & dual AC power & internal V.90 modem

- **LX-4008T-112DCF LX-4000T** with (8) RS232 RJ45 ports, & dual DC (36-72V) power & internal modem V.90

- **LX-40016T-001ACF LX-4000T** with (16) RS232 RJ45 ports, & single AC power

- **LX-40016T-002ACF LX-4000T** with (16) RS232 RJ45 ports, & dual AC power

- **LX-40016T-012DCF LX-4000T** with (16) RS232 RJ45 ports, & dual DC (36-72V) power

- **LX-40016T-101ACF LX-4000T** with (16) RS232 RJ45 ports, & single AC power & internal V.90 modem

- **LX-40016T-102ACF LX-4000T** with (16) RS232 RJ45 ports, & dual AC power & internal V.90 modem

- **LX-40016T-112DCF LX-4000T** with (16) RS232 RJ45 ports, & dual DC (36-72V) power & internal modem V.90

- **LX-40032T-001ACF LX-4000T** with (32) RS232 RJ45 ports, & single AC power

- **LX-40032T-002ACF LX-4000T** with (32) RS232 RJ45 ports, & dual AC power

- **LX-40032T-012DCF LX-4000T** with (32) RS232 RJ45 ports, & dual DC (36-72V) power

- **LX-40032T-101ACF LX-4000T** with (32) RS232 RJ45 ports, & single AC power & internal V.90 modem

- **LX-40032T-102ACF LX-4000T** with (32) RS232 RJ45 ports, & dual AC power & internal V.90 modem

- **LX-40032T-112DCF LX-4000T** with (32) RS232 RJ45 ports, & dual DC (36-72V) power & internal modem V.90

- **LX-40048T-001ACF LX-4000T** with (48) RS232 RJ45 ports, & single AC power

- **LX-40048T-002ACF LX-4000T** with (48) RS232 RJ45 ports, & dual AC power

- **LX-40048T-012DCF LX-4000T** with (48) RS232 RJ45 ports, & dual DC (36-72V) power

- **LX-40048T-101ACF LX-4000T** with (48) RS232 RJ45 ports, & single AC power & internal V.90 modem

- **LX-40048T-102ACF LX-4000T** with (48) RS232 RJ45 ports, & dual AC power & internal V.90 modem

- **LX-4048T-112DCF LX-4000T** with (48) RS232 RJ45 ports, & dual DC (36-72V) power & internal modem V.90

The logical interfaces and their module mapping are described in the following table:

Logical Interface	Physical Interface Mapping
Data Input Interface	2 10/100 BASE-TX Ports 8 RS232 RJ45 Ports / 16 RS232 RJ45 Ports 32 RS232 RJ45 Ports / 48 RS232 RJ45 Ports RS232 RJ45 Diagnostic Management Port (RS232 Modem Port)
Data Output Interface	2 10/100 BASE-TX Ports 8 RS232 RJ45 Ports / 16 RS232 RJ45 Ports 32 RS232 RJ45 Ports / 48 RS232 RJ45 Ports RS232 RJ45 Diagnostic Management Port (RS232 Modem Port)
Control Input Interface	Reset Button 2 10/100 BASE-TX Ports 8 RS232 RJ45 Ports / 16 RS232 RJ45 Ports 32 RS232 RJ45 Ports / 48 RS232 RJ45 Ports RS232 RJ45 Diagnostic Management Port (RS232 Modem Port)
Status Output Interface	LEDs, 2 10/100 BASE-TX Ports 8 RS232 RJ45 Ports / 16 RS232 RJ45 Ports 32 RS232 RJ45 Ports / 48 RS232 RJ45 Ports RS232 RJ45 Diagnostic Management Port (RS232 Modem Port)
Power Interface	(Dual) AC Power Input / Dual DC Power Input

3. Roles, Services, and Authentication

The LX-4000T Series provides four different roles and a set of services specific to each of the roles. The LX4000T Series will authenticate an operator by verifying his password and will then explicitly assign him either the Crypto-Officer or User role, depending on his security level (the module implements a permission mechanism). The module provides role-based authentication for all operators. The module can also authenticate Crypto-Officer or User operators by using an authentication server (LDAP, Kerberos, RADIUS, TACACS+, RSA SecurID).

3.1. Roles

The roles of the module include a PPCIBOOT User, Crypto-Officer, and User Role. Services that are available are summarized below. Please see section "Cryptographic Keys, CSPs, and SRDIs" below for additional detail.

PPCIBOOT User

The PPCIBOOT User is responsible for configuring the boot loader.

The following services are provided:

- Establish boot loader session
- Configure boot parameters
- Enable FIPS 140-2 mode
- Disable FIPS 140-2 mode

Crypto-Officer Role

The Crypto-Officer is the administrator of the LX and does the configuration.

 The following services are provided:

- Module service configuration, control, and status
- Serial device connection configuration, control, and status
- MRV sensor and power management configuration, control, and status

Please see *LX-Series Commands Reference Guide* for the complete list of corresponding command-line (CLI) services. Please see *LX-Series Configuration Guide* for the complete description of corresponding GUI services. Note that the GUI calls the CLI services (it generates command-line commands which the module then executes on behalf of the operator).

User Role

The User Role performs a limited set of services to retrieve information or status. This role cannot perform services to configure the box.

The following services are provided:

- Module status
- Connect to a Serial device
- Use ping utility

Please see *LX-Series Commands Reference Guide* for a complete list of services and the permission necessary to access them.

The module allows concurrent users.

3.2. Authentication Mechanisms

PPCIBOOT Password Authentication Mechanism

Role: PPCIBOOT User
Authentication Type: password based authentication
Authentication Data: Iboot User password
The module enforces a 6 character password minimum chosen from the 94 human readable ASCII characters.
The probability of a successful random attempt is $1/94^6$ which is less than 1,000,000
The module can process a maximum of 60 attempts in a minute. The probability of a successful authentication attempt within multiple authentication attempts in a one minute period is $60/94^6$ which is less than 1/100,000

Crypto-Officer and User Username/Password Authentication Mechanism

Role: Crypto-Officer, User
Authentication Type: password based authentication
Authentication Data: Crypto Officer password, User password
The module enforces a 6 character password minimum chosen from the 94 human readable ASCII characters.
The probability of a successful random attempt is $1/94^6$ which is less than 1,000,000

The module can process a maximum of 30,720 attempts in a minute. The probability of a successful authentication attempt within multiple authentication attempts in a one minute period is $30,720/94^6$ which is less than 1/100,000

IKE PSK Authentication Mechanism

Role: Crypto-Officer
Authentication Type: password based authentication
Authentication Data: The IKE protocol pre-shared key
The secret should have a 6 character minimum length chosen from the 94 human readable ASCII characters.
The probability of a successful random attempt is $1/94^6$ which is less than 1/1,000,000.
The module can process a maximum of 61,440 attempts in a minute.
The probability of a successful authentication attempt within multiple authentication attempts in a one minute period is $61,440/94^6$ which is less than 1/100,000

SSH Transport Protocol Host Authentication Mechanism

Role: Crypto-Officer, User
Authentication Type: public key based authentication
Authentication Data: ssh_host_rsa_key, ssh_host_rsa_key.pub, ssh_host_dsa_key, ssh_host_dsa_key.pub
A 1024-bit DSA key has at least 80-bits equivalent strength. The probability of a successful random attempt is $1/2^{80}$, which is less than 1/1,000,000
A 2048-bit RSA key has at least 112-bits of equivalent strength. The probability of a successful random attempt is $1/2^{112}$, which is less than 1/1,000,000
The module can process a maximum of 60 attempts in a minute. The probability of a successful authentication attempt within multiple authentication attempts in a one minute
period for a 1024-bit DSA key is $60/2^{80}$ which is less than 1/100,000
The probability of a successful authentication attempt within multiple authentication attempts in a one
minute period for a 2048-bit RSA key is $60/2^{112}$ which is less than 1/100,000

SSH Authentication Protocol Public Key Mechanism

Role: Crypto-Officer, User
Authentication Type: public key based authentication
Authentication Data: Operator's private key, Operator's private key passphrase, Operator's public key (RSA/DSA)
A 1024-bit DSA key has at least 80-bits equivalent strength. The probability of a successful random attempt is $1/2^{80}$, which is less than 1/1,000,000
A 2048-bit RSA key has at least 112-bits of equivalent strength. The probability of a successful random attempt is $1/2^{112}$, which is less than 1/1,000,000
The module can process a maximum of 60 attempts in a minute. The probability of a successful authentication attempt within multiple authentication attempts in a one minute
period for a 1024-bit DSA key is $60/2^{80}$ which is less than 1/100,000
The probability of a successful authentication attempt within multiple authentication attempts in a one
minute period for a 2048-bit RSA key is $60/2^{112}$ which is less than 1/100,000

Cluster Authentication Mechanism

Role: Crypto-Officer
Authentication Type: password based authentication
Authentication Data: Cluster Secret
The module enforces a 16 character password minimum chosen from the 94 human readable ASCII characters.
The probability of a successful random attempt is $1/94^{16}$ which is less than 1,000,000
The module can process a maximum of 30,720 attempts in a minute.
The probability of a successful authentication attempt within multiple authentication attempts in a one minute period is $30,720/94^6$ which is less than 1/100,000

Authentication Server Mechanisms

RADIUS
Role: Authentication Server User
Authentication Type: password based authentication

Authentication Data: RADIUS secret
The module enforces a 6 character password minimum chosen from the 94 human readable ASCII characters.
The probability of a successful random attempt is 1/94^6 which is less than 1,000,000
The module can process a maximum of 30,720 attempts in a minute.
The probability of a successful authentication attempt within multiple authentication attempts in a one minute
period is 30,720/94^6 which is less than 1/100,000

TACACS+
Role: Authentication Server User
Authentication Type: password based authentication
Authentication Data: TACACS+ secret
The module enforces a 6 character password minimum chosen from the 94 human readable ASCII characters.
The probability of a successful random attempt is 1/94^6 which is less than 1,000,000
The module can process a maximum of 30,720 attempts in a minute.
The probability of a successful authentication attempt within multiple authentication attempts in a one minute
period is 30,720/94^6 which is less than 1/100,000

RSA SecurID
Role: Authentication Server User
Authentication Type: password based authentication
Authentication Data: RSA SecurID secret
The probability of a successful random attempt is 1/255^16 which is less than 1,000,000
The module can process a maximum of 30,720 attempts in a minute.
The probability of a successful authentication attempt within multiple authentication attempts in a one minute period is 30,720/255^16 which is less than 1/100,000

LDAP
Role: Authentication Server User
Authentication Type: public key based authentication
Authentication Data: LDAP primary and secondary public CA keys
A 1024-bit DSA key has at least 80-bits equivalent strength. The probability of a successful random attempt is 1/2^80, which is less than 1/1,000,000
A 2048-bit RSA key has at least 112-bits of equivalent strength. The probability of a successful random attempt is 1/2^112, which is less than 1/1,000,000

The module can process a maximum of 30,720 attempts in a minute.
The probability of a successful authentication attempt within multiple
authentication attempts in a one minute period for a 1024-bit DSA key
is $30{,}720/2^{80}$ which is less than 1/100,000
The probability of a successful authentication attempt within multiple
authentication attempts in a one minute period for a 2048-bit RSA key
is $30{,}720/2^{112}$ which is less than 1/100,000

Kerberos
    Role: Authentication Server User
    Authentication Type: password based authentication
    Authentication Data: Kerberos secret
    The secret is derived from the password which should have 6 character
    minimum length chosen from the 94 human readable ASCII
    characters.
    The probability of a successful random attempt is $1/94^{6}$ which is less
    than 1,000,000
    The module can process a maximum of 30,720 attempts in a minute.
    The probability of a successful authentication attempt within multiple
    authentication attempts in a one minute period is $30{,}720/94^{6}$ which is
    less than 1/100,000

3.3. Algorithms

The LX supports the following cryptographic algorithms.

Approved cryptographic algorithms (LX-Series Algorithm Core)

Symmetric Key Algorithms

Algorithm	Modes	Key Size
AES (Cert. #854)	ECB, CBC, CFB, CTR	128, 192, 256
Triple-DES (Cert. #704)	ECB, CBC	112, 168

Hashing Algorithms

SHA-1, SHA-256 (Cert. #848)

Message Authentication Algorithms

HMAC SHA-1, HMAC SHA-256

(Cert. #471)

Asymmetric Key Algorithms

Algorithm	Key Size
RSA (PKCS 1.5) (Cert. #408)	1024, 2048
DSA (Cert. #308)	1024

RNG Algorithms

ANSI X9.31 (Triple-DES 2 Key) (Cert. #489)

Approved cryptographic algorithms (LX-Series Algorithm IPSec Core)

Symmetric Key Algorithms

Algorithm	Modes	Key Size
AES (Cert. #855)	CBC	128, 192, 256
Triple-DES (Cert. #705)	CBC	112, 168

Hashing Algorithms

SHA-1, SHA-256 (Cert. #849)

Message Authentication Algorithms

HMAC SHA-1, HMAC SHA-256 (Cert. #472)

Non-FIPS Approved Algorithm

Symmetric Key Algorithms

Algorithm	Modes	Key Size
DES	CBC	64

Asymmetric Key Algorithms

Algorithm	Key Size
RSA encrypt / decrypt (key wrapping, allowed in FIPS mode)	1024, 2048 (key establishment methodology provides 80 and 112 bits of encryption strength)

Hashing Algorithms

MD5

Key Establishment Algorithms

Algorithm	Key Size
Diffie-Hellman (allowed in FIPS mode)	1024, 2048, 4096 (key establishment methodology provides between 80 and 150 bits of encryption strength)

RNG Algorithms

Non-Approved RNG

Key Generation

The module implements the ANSI X9.31 A.2.4 based PRNG. All key generation functions use the approved PRNG implementation.

4. Setting FIPS 140-2 Mode

The module images are pre-installed in the flash and new versions of software are shipped on CDs. All shipping occurs via a reputable courier service. The administrator should also inspect to make sure the boxes have not been tampered with or damaged upon receiving the modules, which could indicate a security compromise. Please see "Installing the LX-4000T Series" for additional detail about how to install the module.

4.1. Prerequisites

The following requirements must be met to use the product in a FIPS 140-2 compliant configuration:

- You must use the FIPS 140-2 validated versions of the LX linuxito and ppciboot software. *Only specific versions of the LX software are tested by an accredited cryptographic module test lab.*

- You must be running the software on the FIPS 140-2 tested LX-Series platform.

- FIPS 140-2 mode must be enabled on the LX-Series FIPS 140-2 validated unit(s).

- If you intend to use SNMP with FIPS 140-2, you must use the SNMP V3 version.

- You must place the provided tamper-evident labels in the proper locations.

4.2. Notes and Restrictions

- The default subscriber InReach password must be changed.

- The default ppciboot password must be changed.

- The default system password must be changed.

- All configured passwords must be greater than or equal to 6 characters in length.

- All configured keys must be entered in hexadecimal format using the prefix "0x".

- If using an SNMP NMS or SNMP MIB browser, the application must support SNMPV3 and must support AES encryption. By default SNMP is disabled for security reasons. SNMP V3 must be enabled and configured fully on the LX in order to function with the NMS. Further, SNMP V3 must be configured to use only FIPS-Approved and Allowed algorithms.

- SSH Clients must support sshV2, AES or 3DES ciphers, and HMAC-SHA1 or HMAC-SHA1-96 message authentication codes.

- Telnet, TCP pipe, TFTP, Broadcast groups services can be used only if secured via IPSec tunnel.

- Use of Expect and TCL scripts is not allowed.

4.3. Applying Tamper Evident Labels

NOTE: To be FIPS 140-2 compliant, you must apply the tamper-
       evident labels before you power on and configure the LX unit.

Once the LX has been configured in FIPS 140-2 mode, the cover cannot
be removed without signs of tampering. Applying tamper-evident
labels to the LX unit will prevent anyone from opening the unit
without your knowledge.

To seal the cover of the LX, apply a tamper-evident label as follows:

1. Clean the LX surface of any grease or dirt before you apply the
    tamper-evident labels.

2. Apply two labels each to the bottom left and right sides of the unit,
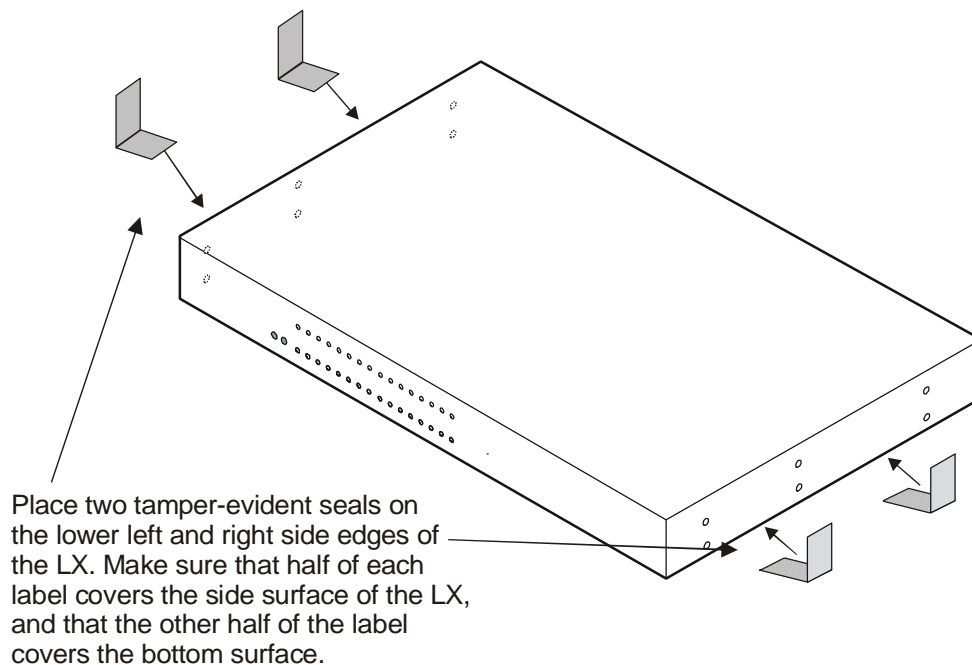   as shown in Figure 1.

Place two tamper-evident seals on
the lower left and right side edges of
the LX. Make sure that half of each
label covers the side surface of the LX,
and that the other half of the label
covers the bottom surface.

Figure 1 – Location of the Tamper Evident Labels

3. Record the serial numbers of the labels you attached to the LX unit.

4. Allow 24 hours for the adhesive in the tamper-evident labels to cure.

NOTE: You should periodically check the labels to ensure that no one
       has tampered with the unit.

4.4. Making Sure Your Software is FIPS 140-2 Validated

Do the following to determine if the software you are running has been FIPS 140-2 validated:

1. Log into the CLI.

2. Enter the `show version` command at the **InReach:0 >** prompt; for example:

   InReach:0 > `show version`

The Show Version screen appears, with the relevant fields highlighted:

```
Linux Kernel Version:                             x.x.x.x
Linux In-Reach Version:                                 x
Software Version (Runtime):         x.x.x.x (FIPS 140-2)
Software Version (Flash):           x.x.x.x (FIPS 140-2)
Ppciboot Version:                   x.x.x.x (FIPS 140-2)
```
Figure 2 – Show Version Screen

If the software you are running has been FIPS 140-2 validated, the word (FIPS 140-2) appears to the right of the Software Version number and the Ppciboot Version number. If (FIPS 140-2) does not appear, your software has not been validated.

4.5. Enabling FIPS 140-2 Mode of Operation

IMPORTANT!
If you want to configure your unit to run FIPS 140-2 Mode of Operation, you must do so ***before*** you attempt to configure the unit over and above the default settings. The act of enabling FIPS 140-2 mode will default the unit's configuration.
When FIPS 140-2 is enabled, the configuration file is returned to defaults. Therefore, if you fully configured your unit and then turned on FIPS 140-2, your configuration will return to factory defaults. FIPS 140-2 mandates this to ensure that any passwords with fewer than six characters are purged, and that all unsupported applications are disabled.

NOTE: If you enable FIPS 140-2 Security, option `[1] Boot from Network` is set to `Flash Only` automatically. You can only update from the CLI or GUI while FIPS 140-2 is enabled. Option `[4] Update ppciboot Firmware` is disabled when FIPS 140-2 is enabled.

The following passwords must be at least six characters long:

- Subscriber
- Config
- ppciboot
- Radius Secret
- TACACS+ Secret
- Kerberos Secret
- PAP/CHAP Outgoing Secret
- SSH Host Authentication Public Key must be at least 1024 bits.
- SSH Operator's Public Key must be at least 1024 bits.

The `FIPS 140-2 Security` option lets you enable or disable FIPS 140-2 mode of operation.

```
                     Main Menu


        [1] Boot from:                        Flash only
            Image currently in flash:         4.1.4 (FIPS 140-2)
        [2] Time Out, in seconds (0=disabled): 8
        [3] IP Configuration Menu
        [4] Update Ppciboot Firmware
        [5] Ethernet Network Link:            auto
        [6] Change PPCiBoot password
        [7] FIPS 140-2 Security:              yes
        [9] ppciboot image name:              ppciboot.img
        [0] software image name:              linuxito.img

        [*] Reset to System Defaults
        [D] Downgrade Ppciboot Firmware
        [S] Save Configuration
        [B] Boot System

        Make a choice:
```

To enable or disable FIPS 140-2 security:

1. Press the number 7 (FIPS 140-2 Security). The following prompt appears:

   `Enabling FIPS security will reset run-time configuration to defaults. Are you sure? (y/n):`

2. If you select `y` (this defaults the flash immediately), a `Resetting Linux Configuration` message appears, and the Main Menu reappears after a few seconds. If you select `n`, the Main Menu reappears immediately.

3. If FIPS 140-2 is already enabled and you want to disable it, press `7` (`FIPS 140-2 Security`) from the Main Menu.

4. Press `B` to Boot the system. Do this only after you have configured the ppciboot options and saved the configuration.

4.6. Changing the Default ppciboot Password

After enabling FIPS 140-2, you must enter a new ppciboot password of greater than six characters.

The `Change ppciboot Password` option lets you change the ppciboot password for the unit. To change the ppciboot password:

1. Press the number 6 (`Change ppciboot Password`). The following prompt is displayed:

   Enter your current ppciboot password:

   Enter the current ppciboot password at the above prompt. After you have entered the current ppciboot password, the following prompt is displayed:

   Enter your NEW password: :

2. Enter the new ppciboot password at the above prompt. The password must be greater than six characters long.

   After you have entered the new ppciboot password, the following prompt is displayed:

   Re-enter your NEW password:

Re-enter the new ppciboot password at the above prompt. A confirmation message is displayed.

4.7. Changing the Default Subscriber Password

It is widely known that the default password for the **InReach** user is **access**. If an unauthorized user knew this username/password combination, he/she could log on to your LX unit. For this reason, you must change the InReach user's password to something other than **access**. The password must be at least six characters long.

Changing the Default Password for the InReach User

Do the following to change the User-level password of the **InReach** User:

1. Access the Configuration Command Mode.

2. Access the Subscriber Command Mode for the **InReach** subscriber. You do this by entering the `subscriber` command with **InReach** as the command argument; for example:

   Config:0 >> `subscriber InReach`

3. Enter the `password` command at the **Subs_InReach** >> prompt; for example:

   Subs_InReach:0 >> `password`

4. Enter a new User password at the **Enter your NEW password:** prompt. The password will be displayed as asterisks, as in the following example:

   Enter your NEW password:*************

5. Re-enter the new User password at the **Re-Enter your NEW password:** prompt. The password will be displayed as asterisks, as in the following example:

   Re-Enter your NEW password:*************

Changing the Default Configuration Password

It is also widely known that the default Superuser password is **system**. To reduce the risk of an unauthorized user gaining access to the Superuser Command Mode, you must change this password to something other than **system**. The password must be at least six characters long.

To change the Configuration password for the LX unit, do the following:

1. Access the Configuration Command Mode.

2. Enter the password command at the **Config:0 >>** prompt; for example:

   Config:0 >>`password`

3. Enter a new Superuser password at the **Enter your NEW password:** prompt. The password will be displayed as asterisks, as in the following example:

   Enter your NEW password:***************

4. Re-enter the new Superuser password at the **Re-Enter your NEW password:** prompt. The password will be displayed as asterisks, as in the following example:

   Re-Enter your NEW password: ***************

4.8. FIPS 140-2 Mode Console Access

When the LX is in FIPS 140-2 mode telnet is not allowed. Therefore, you must ssh to the unit in Version 2 mode.

```
ssh -l InReach 10.10.10.10
```

If non-FIPS 140-2 approved algorithms are being used, please see and edit the `/etc/ssh/ssh_config` file on your host system.

4.9. Applications Unsupported in FIPS 140-2 Mode of Operation

Listed below are all the unsupported FIPS 140-2 protocols and features, which are disabled when FIPS 140-2 mode of operation is enabled on the LX software. Features which have unsupported reasoning "Must be secured with IPSEC" are allowed to be used in FIPS 140-2 mode of operation when an IPSec tunnel has been established.

Unsupported FIPS Protocols and Features

Feature	Impact	Reason
Telnet client/server	Limited	Must be secured with IPSEC
rlogin client	Disabled	Passwords are passed in plaintext
Web GUI	Limited	Customer is required to run a FIPS 140-2 approved JRE on host machine
SNMP v1 & v2	Disabled	Community strings are passed in plaintext
SSH V1 Client / Server	Disabled	Security flaws / known vulnerabilities
Passwords/ Secrets less than 6 characters	Disabled	Due to FIPS 140-2 max authentication fail attempts
Linux shell access	Restricted	Disabled access to secret and private keys
Boot or load software image from network	Disabled	FIPS 140-2 requires DSA signatures on images, units must boot from FLASH
Updating ppciboot.img from ppciboot menu	Disabled	FIPS 140-2 requires ppciboot to be updated from runtime software via CLI or GUI
Login mode shell	Disabled	Unfettered access
Broadcast Groups	Limited	Must be secured with IPSEC
Fingerd	Disabled	Allows anyone to see who is logged in
Boot config from network (tftp)	Limited	Must be secured with IPSEC
Save config to network (tftp)	Limited	Must be secured with IPSEC
No authentication	Disabled	Insecure
Dedicated Services	Disabled	Passwords are passed in plaintext
TCP Pipe	Limited	Must be secured with IPSEC

IPSEC IKE v2	Disabled	Not supported in FIPS 140-2 mode
Expect Scripting	Disabled	Considered untrusted software

4.10. Upgrading Software

The `ppciboot.img.sign` and `linuxito.img.sign` digital signature files are used to authenticate load images during loading. Place these files on the TFTP server. The LX unit will download them automatically.

Refer to "How to Upgrade the Software" in the *LX-Series Configuration Guide* for more information on upgrading the software.

4.11. FIPS 140-2 JCE Module Commands

NOTE: These commands apply only if a Crypto-Officer or a User wants to use the GUI in FIPS 140-2 mode. The module provides a GUI in the form of a Java applet that is downloaded from the module to a web browser using HTTP. The applet communicates with the module using TLS. The applet is not part of the module. The applet authenticates operators (according to module configuration) and accesses module services (according to role) by tunneling CLI commands to the module.

NOTE: You can purchase FIPS 140-2 compliant JCE modules from two vendors. The vendors are listed below, along with the specific JCE Module name.

- IBM – IBMJCEFIPS
- RSA – JSafeJCE

NOTE: These commands are available only when the LX is running in FIPS 140-2 Mode.

A new FIPS 140-2 JCE Module command allows you to name the web server FIPS 140-2 JCE Module. You can access it in the Configuration Command Mode.

Configuring a Web Server FIPS 140-2 JCE Module Name

Use the following command to configure a Web Server FIPS 140-2 JCE Module name. The module name is set by the module vendor. For example, if you are using RSA's JSafe cryptographic module, the module name would be `JSafeJCE`. Enter `no web_server fips jcemodule` to reset to the default, which is "null". The module name can be up to 16 characters long.

Config:0>> `web_server fips jcemodule <module_name>`

Examples

Config:0>> `web_server fips jcemodule JSafeJCE`

Config:0>> `no web_server fips jcemodule`

4.12. Viewing the Web Server FIPS 140-2 JCE Module Name

Use the `show web characteristics` command to display the Web Characteristics Screen. An example of this screen follows, with the new `Web JCEModule` field highlighted:

```
Time:                              Fri, 28 Jan 2005 13:52:48 US/EASTERN
Web Server:              Enabled  Web Server Port:                  80
Web Server Timeout:           20  Web Encrypt:                Disabled
Web Banner:              Enabled  Web JceModule:           JsafeJCEFIPS
```

5. Definition of SRDIs Modes of Access

This section specifies the LX's Security Relevant Data Items.

5.1. Cryptographic Keys, CSPs, and SRDIs

While operating in a level 2 FIPS compliant manner, the LX-4000T Series contains the following security relevant data items:

Security Relevant Data Item	SRDI Description
IPSec manual mode keys	The following keys are used/generated in IPSec manual mode: IPSec AH protocol – integrity key (HMAC) IPSec ESP protocol – encryption key (TDES/AES), integrity key (HMAC) All of the above are stored in flash.
IKE/IPSec keys	The following keys are used/generated when IKE is used with IPSec: IKE (phase 1) – IKE protocol pre-shared key (HMAC), IKE protocol DH private key, IKE protocol DH public keys, IKE protocol authenticated keying material IKE (phase 2) – IKE protocol PFS – DH private key, IKE protocol PFS – DH public key, IKE/IPsec AH protocol – integrity key (HMAC), IKE/IPsec ESP protocol – encryption key (TDES/AES), IKE/IPsec ESP protocol – integrity key (HMAC) The IKE protocol pre-shared key is stored in flash. All other IKE/IPSec keys are stored in RAM.
SSH transport protocol keys	The following keys are used/generated by the SSH transport protocol: SSH transport protocol – DH private key, DH public keys, integrity key (HMAC), encryption key (TDES/AES), module's host authentication private key (DSA/RSA), module's host authentication public key (DSA/RSA), known

	host authentication public keys (DSA/RSA), authorized host authentication public keys (DSA/RSA) The DH, integrity, and encryption keys are stored in RAM. All other SSH transport keys are stored in flash.
SSH authentication protocol keys	The following keys are used/generated by the SSH authentication protocol: SSH authentication protocol – publickey method – operator's private key (DSA/RSA), publickey method – operator's private key passphrase, publickey method – operator's public key (DSA/RSA) All SSH authentication protocol keys are stored in flash.
Web Server RSA 1024-bit private key	Used for Web server authentication and key transport. Stored in flash.
Web Server RSA 1024-bit public key	Used for Web server authentication and key transport. Stored in flash.
Cluster Secret	Shared secret used to authenticate cluster members after establishing a TLS connection. Stored in configuration file in flash.
User passwords	User passwords. Stored in configuration file in flash.
Crypto Officer password	Password used to authenticate Crypto Officer. Stored in configuration file in flash.
Iboot User password	Password used to authenticate Iboot User. Stored in flash.
SNMP v3 AES encryption key	Key used for SNMP v3 encryption. Stored in flash.
SNMP v3 HMAC integrity key	Key used for SNMP v3 integrity. Stored in flash.
Outgoing PAP Secret	Used in PPP authentication. Stored in configuration file in flash.
Outgoing CHAP Secret	Used in PPP authentication. Stored in configuration file in flash.
RADIUS secret	Shared secret used with authentication server. Stored in configuration file in flash.
TACACS+ secret	Shared secret used with authentication server. Stored in configuration file in flash.

Kerberos secrets	Shared secrets used with authentication server. Stored in configuration file in flash.
LDAP primary and secondary CA public keys	Public keys used with authentication server. Stored in configuration file in flash.
Cluster TLS Diffie-Hellman private key	Diffie-Hellman private key used in Clustering. Stored in RAM.
Cluster TLS Diffie-Hellman public key	Diffie-Hellman public key used in Clustering. Stored in RAM.
Web Server Session encryption key	Web server session encryption key. Stored in RAM.
Web Server Session integrity key	Web server session integrity key. Stored in RAM.
Cluster TLS Session key	Cluster session encryption key. Stored in RAM.
Cluster TLS Session integrity key	Cluster session integrity key. Stored in RAM.
RSA SecurID Secret	Shared secret of RSA SecurID. Stored in Flash.
DSA public key for firmware load	DSA public key used in signature verification when loading firmware. Stored in flash.
Approved PRNG initial seed and seed key	Used to initialize approved PRNG. Stored in flash.
Runtime approved PRNG seed and seed key	The runtime seed and seed key values stored in RAM

The following matrix defines the set of services to the CSP of the module, providing information on reading, writing, and deleting.

The matrix uses the following convention:

- x: All SRDIs of the indicated type are used/generated by the service using its associated protocol messages
- p: Only SRDIs of the indicated type that are stored in flash are used by the service

SRDI/Role/Service Access Policy	Security Relevant Data Item	GUI TLS (RSA for server authentication and key establishment) Protocol SRDIs	lboot User password	IKE/IPSec IPv4/IPv6 Protocol SRDIs	IPSec IPv4/IPv6 Protocol SRDIs	MRV Cluster TLS (Using Diffie-Hellman) Protocol SRDIs	PPP IPv4 Protocol SRDIs	Operator (subscriber) passwords, DSA public key for firmware load	RADIUS secret, TACACS+ secret	SNMPv3 Protocol SRDIs	SSH Protocol Keys and CSPs	Kerberos, LDAP, SecurID SRDIs
Role/Service												
Crypto-Officer Role												
Module service configuration, control, and status Additional detail:		x		x	x	x	x	x	x	x	x	x
• Cluster configuration, control, and status									x	x		
• IKE/IPSec				x								
• IPSec					x							
• IPv6 CLI (subset of PPP/IPv4 interfaces, but include "reload" and "show"/LEDs)								x				x
• PPP							x	x				x
• PPP/IPv4 CLI o "reload" initiates self-tests o "show" and LEDS provide status o "update ppciboot" and "update software" load firmware								x				x
• SNMPv3										x		
• SSH and TLS (between modules)						x					x	
• TLS (between applet and module)		x										
• User/CO-defined Expect and TCL scripts (not allowed in FIPS mode)												

Serial device connection configuration, control, and status													
MRV sensor and power management configuration, control, and status													
Iboot User Role													
Boot loader session interfaces			x										
Configure boot parameters													
Enable FIPS 140-2 mode		p	p	p	p	p	p	p	p	p	p	p	
Disable FIPS 140-2 mode													
Authentication Server User Role													
Authenticate operator									x			x	

Note that User role services are not listed separately in the table above. User role services are defined as a subset of CO role services. The module supports a permission mechanism that determines what services a User may access. Services are accessible based on permissions assigned to the User by the CO.

There are six different permissions that may be assigned to a User and map to services as follows:

-

User	Basic permission which has some CLI commands (clear, cluster, connect, dial, exit, menu, message, monitor, no, password, pause, ping, ppp, rlogin, show, ssh, telnet, terminal, zero) along with ping, telnet
Outlet	Adds the ability for "outlet" commands
Outlet configuration	Adds the ability to configure names of outlets
Read	Adds the ability to do all "show" commands
shell	Adds the ability to access the shell
Superuser	Gives the user access to everything including all configuration commands

A User that has been assigned the superuser permission is considered the CO.

6. Mitigation of Other Attacks

This section is not applicable.