Telkonet

G3 Series iBridge/eXtender

Security Policy

March 7, 2006

Telkonet Communications, Inc.
20374 Seneca Meadows Pkwy
Germantown, MD 20876
Telephone: 240-912-1800
FAX: 240-912-1839
www.telkonet.com

Section 1 Introduction

The Telkonet system of components is described in two security policy documents. The first one is the Gateway security policy and the second one is the iBridge/eXtender security policy.

The Telkonet G3 Series iBridge/eXtender uses power line communications (PLC) technology to deliver broadband internet to a building's existing electrical wiring. The system consists of four components: The Telkonet Gateway, Telkonet iBridge, Telkonet eXtender and Telkonet Coupler. These components are hardware devices containing firmware. The Coupler is an interface device that contains no security components and is outside the cryptographic boundary.

1.1 Purpose

The purpose of this security policy is to provide the operator with a specification of the Telkonet G3 Series iBridge/eXtender and the rules under which the module operates.

This document concentrates on the description of the iBridge and eXtender.

1.2 Description

The iBridge and eXtender are each enclosed in a metal case, which defines the physical boundary for each unit. The logical boundary is the cryptomodule itself, which is loaded into FLASH at the same time as the firmware (version 2.12 and 2.41). The iBridge and eXtender are FIPS 140-2 level-2, multi-chip standalone modules. The module only operates in compliance with FIPS Pub 140-2. No other mode of operation is available.

The cryptographic algorithms used in the module are:

FIPS Approved	AES, CBC, 256-bit key	Cert # (223)
Non-FIPS Approved	RSAES-OAEP, 1024-bit key for key wrapping	

1.2.1 Identification

Hardware module numbers:

iBridge Hardware Models: iB8200, iB8000, iB8201, iB8001, iB8011, iB8211 (Firmware version 2.12 and 2.41)

eXtender Hardware Models: X7000, X7001, X7200, X7201,X7011, X7211 (Firmware version 2.12 and 2.41)

1.2.2 Interfaces

iBridge: Power interface, 100-240 VAC, 0.25 Amps

Power line carrier interface (via Power interface), IEC 320 AC line cord

Ethernet interface: RJ-45 10/100 base-T.

Extender Power interface, 100-240 VAC, 0.25 Amps

Power line carrier interface, 75 Ohm F-type connector

Ethernet interface: RJ-45 10/100 base-T

1.2.3 System Overview and Configuration

The Gateway is a self-contained unit that bridges data between the Ethernet and PLC media. It is also the hub of the PLC network and the central management point for all units on the network, including iBridges and eXtenders.

The PLC signal generated is routed to the main power service entry via the F connector to the coupler. This allows the Telkonet solution to couple into the low voltage and multi-phase environments found in commercial buildings.

A broadband proprietary protocol bridges data traffic from the Powerline interface to the Ethernet interface. The Gateway can handle up to 1024 iBridges, each of which could connect to a PC or a hub on the Powerline for a total of 4096 end users (PCs).

The Couplers and eXtenders (also called repeaters or secondary gateways) are used to boost signals between the iBridges and the Gateway on the Powerline network. The eXtender may be detected by the Gateway either on the Powerline or on the Ethernet. If the extenders are on the Ethernet, then the communication between the eXtender and the Gateway goes through the Ethernet over 10/100 Mbps Ethernet. A total of 63 eXtenders may be supported by the Gateway in a network.

The Telkonet iBridge in conjunction with the Gateway provides the enhanced communications and management functions required by enterprise customers.

There is no user management software (CLI, Web, or SNMP) on the iBridge. It is managed via the Gateway. All configuration and status/statistics information is passed between the Gateway and the iBridge and can be viewed from the Gateway.

The iBridge, and the eXtenders are firmware upgradeable. The iBridge and the eXtender are upgraded by the Gateway where all firmware is kept. The firmware for the iBridge and eXtender is kept in the Gateway's own firmware. The iBridge and eXtender automatically downloads its firmware from the Gateway if the corresponding stored image revision does not match the image revision in the Gateway.

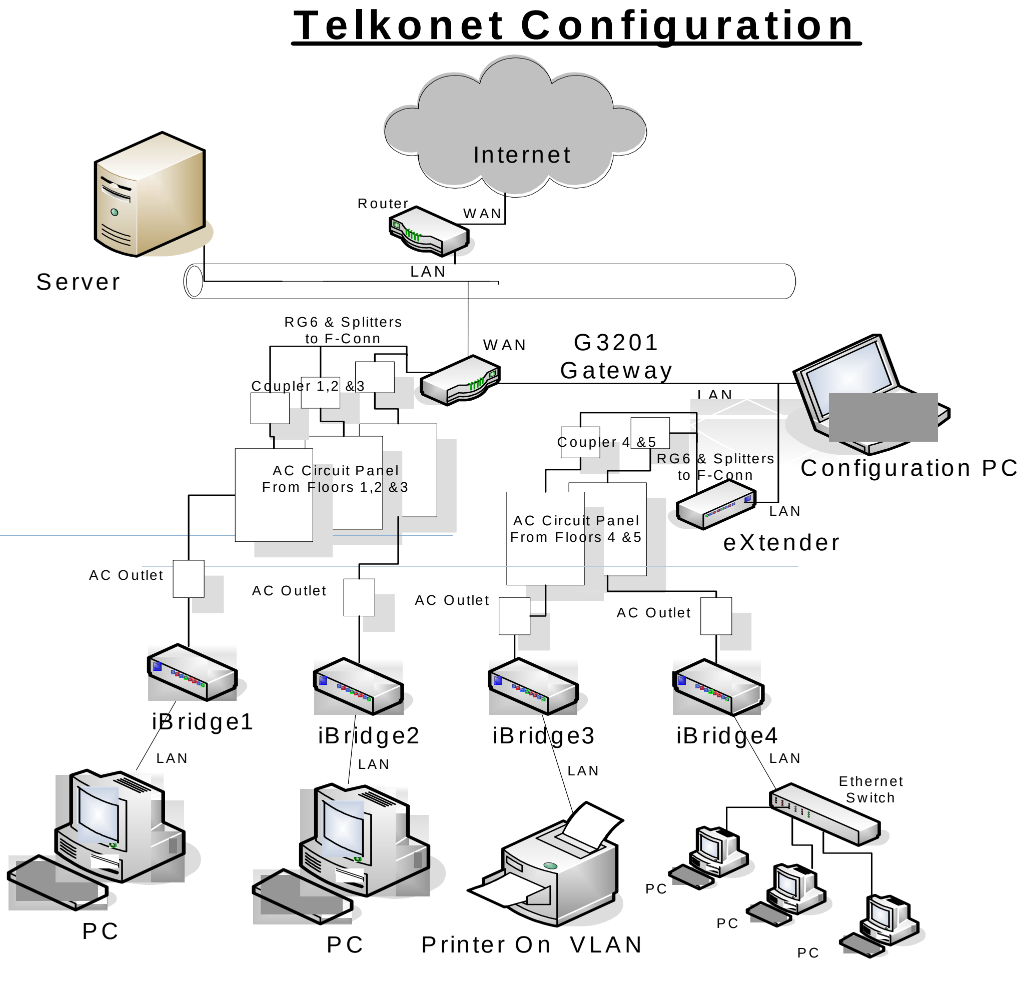


Figure 3

1.3 Scope

The scope of this security policy includes the identification of the Series iBridge/eXtenders, identification and authentication and access control policy, a physical security policy and mitigation against other attacks policy.

Section 2 Identification and Authentication Policy

The Telkonet G3 Series iBridge/eXtender employs role based authentication. A crypto-officer and user role is supported. The module does not support a maintenance role.

The user role is assumed by the module when sending and receiving encrypted packets. The only service available to the user is the ability to transmit data through the network.

The user is authenticated by having knowledge of the secret AES key. The "users" are the iBridge and the eXtender who must share the same AES key as the Gateway. If a Gateway and another appliance have different keys, all communication to and from the offending appliance is dropped by the Gateway. A reset must occur and the correct key must be entered before communications can begin.

The crypto-officer role performs all module security functions and configures the module for use within the network. The crypto-officer must operate within the rules specified in section 3.

The Crypto Officer role is assumed by entering a name and password. The CO password is a minimum of 8 characters long (alpha-numeric). The cardinality of the set of characters is 94. Approximately 30 attempts can be made to guess the module password per minute. (It takes approximately 2 seconds to enter a password. The 2 seconds is based on an average time of 30 unsuccessful attempts.) The probability that the correct guess could be made is 4.92 * 10^-15 which is less than 1/1,000,000. In addition the password is hashed with MD5 to obscure its storage in memory.

Role	Type of Authentication	Authentication Data	Strength
Crypto-officer	Role Password	8 minimum from 92-character ASCII set (printable characters except for space and '^')	92^8
User	Role Knowledge of Secret Key	256 bit key	2^256

Table 1 Roles

The Crypto Officer role is assumed by entering a name and password. The CO password is a minimum of 8 characters long (alpha-numeric). The cardinality of the set of characters is 94. Therefore the probability that the password could be guessed is 1.64 * 10^ -16. This is less than 1/1,000,000. In addition the password is hashed with MD5.

2.1 Series iBridge/eXtender Services

Services provided by the Series iBridge/eXtender are contained in Table 2 below.

Role	Service
Crypto-officer	Configuration
Crypto-officer	Key Entry
Crypto-officer	Key Distribution
Crypto-officer	Self-test
Crypto-officer	Show status
Crypto-officer	Key Zeroization
User	Encryption
User	Decryption

Table 2 Roles and Services

The Telkonet G3 Series iBridge/eXtender employs the AES algorithm in CBC mode to encrypt/decrypt, using a 256-bit secret key, all payload traffic between units.

Service	**Role**	**Key/CSP**	**Storage**	**Access***
Authentication	C-O	Password	FLASH	W/E
Authentication	User	Secret Key	FLASH	E
Key Entry	C-O	AES Secret Key	FLASH	W
Key Entry Key Entry	C-O	RSA Private Key RSA Public Key	iBridge FLASH eXtender FLASH	W W
AES Encryption	User	AES Secret Key	FLASH	E
AES Decryption	User	AES Secret Key	FLASH	E
RSA Decryption	User	RSA Private Key	iBridge FLASH	E
Self-Test	C-O	None	N/A	E
Show Status	C-O	None	N/A	R

Table 3 – Access to Services

*R-Read, W-Write, E-Execute

2.2 Key Utilization

The Secret key may be distributed to the iBridge and eXtender by either of two methods:

1. Secret key manually loaded into the Gateway by the crypto-officer may be transported to the iBridge and eXtender units using RSAES-OAEP encryption. This method is only available if the iBridge/eXtender already has a valid secret key, and therefore is a re-key method and not applicable for establishing an initial key.

2. The crypto-officer may manually load the secret key into each individual unit. If the unit does not have a valid secret key (e.g. the key has been zeroized) this is the only option for loading the key.

The network key is not viewable by the crypto-officer and must be changed at regular intervals. All units in the Telkonet G3 Series iBridge/eXtender network must share the same network key.

The network uses an RSA public/private key pair to encrypt the secret key during re-keying over the network PLC. The secret key is encrypted in the Gateway using the public key and decrypted with the iBridge/eXtender private key. Default asymmetric keys are provided and must be changed by the crypto-officer at initial network configuration.

Access to the module SRDI is restricted to the crypto-officer after authentication by a user-ID and password logon sequence. The user has no access to SRDI.

Key/SRDI	**Type**	**Storage**	**Use**	**Zeroization**
NEK Network	AES 256-bit	FLASH	Traffic encryption/decryption	By C-O command
UpuK Public	RSA 1024-bit	FLASH	Key Transport	By C-O command
UprK Private	RSA 1024-bit	FLASH	Key Transport	By C-O command
C-O Password	Minimum 8-character	FLASH	Authentication	By C-O command

Table 4 Key/SRDI Table

2.3 Key Zeroization

All keys can be zeroized by the crypto-officer using procedures contained in the user guide. There are two methods to zeroize the keys and C-O password. The first is a “delete” command issued by the C-O. The second is the depression of the factory reset button located on the front panel of the Gateway.

2.4 Factory Default

The iBridge/eXtender must be zeroized manually one at a time via the IBMU which is a GUI provided for the management of the iBridge and eXtender

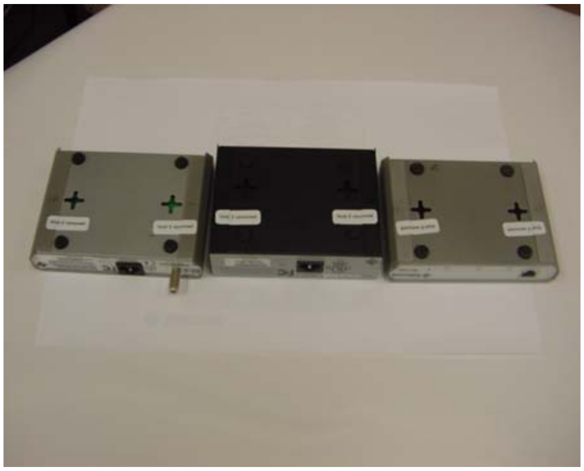
Section 3 Physical Security Policy

3.1 Secure Operation

The Telkonet G3 Series iBridge/eXtenders are contained within metal cases and protected with a tamper evident seal. Physical access to the module by the operator is prohibited; there are no user serviceable components. The module must be returned to the vendor for repair. The hardware meets the FCC Part 15 Class B specification for home or office use.

3.1.1 Tamper Evident Seal

The Telkonet Tamper Label Part Number MLB1R5XR5TPA Gov Tamperproof Label 1.5"X.5" is applied as shown below:



Telkonet expects the eXtender to be used in a controlled space. The iBridge; however, may be externally located outside a controlled space. Telkonet recommends that the modules be inspected regularly for evidence of tampering according to the following schedule.

eXtender	Weekly
iBridge	Daily

3.1.2 Status Indicators

3.1.2.1 IBridge LEDs

The iBridge has 3 LEDs on the front from left to right with the following operating definitions:

- Ethernet – Ethernet Link/Activity - This led closest to the Ethernet RJ48 Port serves as link status and activity led. When data is being passed it blinks.

- PLC - Power Line Carrier Link/Activity – The middle led is to determine the power line Link and Activity. If the iBridge is in a normal operational mode, this LED will behave in one of the following two ways:

  a) **Normally off with occasional quick flashes on.** The iBridge is either in the process of acquiring a link with the Gateway or is unable to link to any Gateway.

b) **Normally on with occasional or frequent flashes off.** The iBridge is linked with the Gateway. Flashes off indicate communications with the Gateway. If traffic is continuously flowing between the iBridge and the Gateway, the LED will continuously flash at a very fast rate.

If the iBridge is in an abnormal operational mode, the PLC LED may behave in a way not described above. Refer to the Telkonet Gateway User Guide for more detailed description.

- Power – This led serves 2 purposes. In normal operation will determine power on to the board. In power on it will show the error code, (see Telkonet Gateway User Guide error codes section for definition).

3.1.2.2 IBridge speed determination

Depress the default test button for **less than** 1 second and release it. The user can watch the LED display on the front panel to determine the current link speed between this iBridge and its Gateway.

The LEDs will all turn off for one second when the request is detected. Zero or more of them will then light up for 2 seconds. All will be off for 1 second and then resume their normal indication.

The LEDs must be read from left to right with the user facing the box. They display the following patterns to indicate the speed:

LED/Speed	1	2	3
(in megabytes/second)	Ethernet	PLC	POWER
< 2			
2 – 2.9	*		
3 – 3.9	*	*	
>= 4	*	*	*

All LEDs flash: Test failed; no Gateway response.

The iBridge must be linked with a Gateway in order to run the test.

3.1.2.3 IBridge Error Indications

Please re word this so that NIST / CSE can understand what you mean.When an iBridge encounters a fatal error the power LED flashes an error code. If the iBridge enters this state immediately upon being powered up, the iBridge hardware has failed and must be replaced. This includes the power-up firmware integrity test.

If the iBridge is linked to a Gateway but has not heard from it in more than 15 seconds, the PLC LED will flash at a 1 Hz rate (½ second on, ½ second off). If the Gateway continues to be unheard, the iBridge will transition to the link down state.

If the iBridge is linked to a Gateway and the iBridge can hear the Gateway but the Gateway cannot hear the iBridge (one-way link), the PLC LED will flash at a 2 Hz rate (¼ second on, ¼ second off).

Other error conditions are indicated by a PLC LED code sequence that repeats every 4 seconds. If the iBridge is linked to a Gateway as the code sequence is displayed, the PLC LED will be normally **on** and flash **off** to display the code. If the iBridge is **not** linked to a Gateway as the code sequence is displayed, the PLC LED will be normally **off** and flash **on** to display the code. The error conditon is indicated by the number of consecutive flashes:

Number of flashes	Error
2	IBridge is disabled (see **Data Transmission**, Section 3.1.2.3
3	NEK is invalid or NEK does not match Gateway's (AES mode only)

Table 6 iBridge LEDs and Description

3.1.2.4 EXtender LEDs.

The eXtender has 3 LEDs on the front from left to right with the following operating definitions:

- Ethernet – Ethernet Link/Activity - This led closest to the Ethernet RJ48 Port serves as link status and activity led. When data is being passed it blinks.

- PLC - Power Line Carrier Link/Activity – The middle led is to determine the power line Link and Activity. If the eXtender is in a normal operational mode, this LED will behave in one of the following two ways:

  a) **Normally off with occasional quick flashes on.** The eXtender is either in the process of acquiring a link with the Gateway or is unable to link to any Gateway.

  b) **Normally on with occasional or frequent flashes off.** The eXtender is linked with the Gateway. Flashes off indicate communications with the Gateway. If traffic is continuously flowing between the eXtender and the Gateway, the LED will continuously flash at a very fast rate.

  If the eXtender is in an abnormal operational mode, the PLC LED may behave in a way not described above. Refer to the Telkonet Gateway User Guide for more detailed description.

- Power – In normal operation this LED is on continuously. If the eXtender experiences a fatal error a code will be displayed

3.1.2.5 eXtender speed determination

Depress the default test button for **less than** 1 second and release it. The user can watch the LED display on the front panel to determine the current link speed between this eXtender and the Gateway.

The LEDs will all turn off for one second when the request is detected. Zero or more of them will then light up for 2 seconds. All will be off again for 1 second and then resume their normal indication.

The LEDs must be read from left to right with the user facing the box. They display the following patterns to indicate the speed:

LED/Speed	1	2	3
(in megabytes/second)	Ethernet	PLC	POWER
< 2			

2 – 2.9	*		
3 – 3.9	*	*	
>= 4	*	*	*

All LEDs flash: Test failed; no Gateway response.

The eXtender must be linked with a Gateway in order to run the test. If the eXtender is linked with the Gateway via ethernet, the test will not run.

3.1.2.6 eXtender Error Indications

Power Supply fold back error are all leds flash off and on as the power supply goes up and down.

When an eXtender encounters a fatal error the power LED flashes an error code. If the eXtender enters this state immediately upon being powered up, the eXtender hardware has failed and must be replaced.

If the eXtender detects more than one Gateway on the network, the PLC LED will flash at a 1 Hz rate (½ second on, ½ second off). This state is latched until the eXtender is rebooted.

Other error conditions are indicated by a PLC LED code sequence that repeats every 4 seconds. If the eXtender is linked to a Gateway as the code sequence is displayed, the PLC LED will be normally **on** and flash **off** to display the code. If the eXtender is **not** linked to a Gateway as the code sequence is displayed, the PLC LED will be normally **off** and flash **on** to display the code. The error conditon is indicated by the number of consecutive flashes:

Number of flashes	Error
3	NEK is invalid or NEK does not match Gateway's (AES mode only)

Continuously (slow)	Detects more than one Gateway on the network.

Table 7 eXtender LEDs and Description

3.1.3 Self Tests

The Telkonet module employs a suite of self-tests to insure proper module operation.

1. Power-up self-tests:

   Firmware integrity test using a 32-bit CRC

   Known Answer Tests on cryptographic algorithms

2. Conditional tests:

   Manual key entry test – An external tool is used to generate the secret key. The secret key has a 3-byte checksum appended at the end. When the CO enters the key into the module, the module will calculate its own checksum and compares with the downloaded checksum. If they do not match, then an error is returned.

3. Callable tests:

   Algorithm KAT

   Power-on self-tests by recycling the power.

Power-up self-tests performed at power-up are initiated automatically. Upon completion, success or failure is indicated on the status LEDs. Data output is inhibited during self-tests. If self-tests fail upon power-up, the unit halts and waits for the operator to reboot the unit.

3.1.4 Basic Security Rules

To ensure secure operation the following security rules must be followed.

1. The Crypto-Officer will not share knowledge of any critical security parameter (passwords, key or key derivatives), with a third party.

2. The Crypto-Officer will change the Network key at regular intervals as prescribed by company policy.

3. The Crypto-Officer will ensure that the tamper-evident seals have been applied according to Telkonet specifications and are inspected at the prescribed intervals.

4. The Crypto-Officer will change the default password when configuring the Gateway for the first time.

5. The Crypto-Officer will configure the module in accordance with guidance found in the User Guide and Policy documents.

6. The Crypto-Officer will zeroize all keys prior to terminating a network configuration or returning a module for repair.

3.2 System Configuration

The system configuration is described more in detail in the Gateway security policy. Only the iBridge/eXtender configuration is described below:

1. Configure the network units (iBridge and eXtender) one at a time.

   a. Connect a PC running Windows 2000 or Windows XP with the IBMU utility installed to the network unit via an Ethernet cable to the LAN interface. Start the IBMU utility.

   b. The IBMU will display a list of discovered units. Select one and authenticate with the default CO password “password”.

   c. Change the CO password.

   d. If the Remote Re-Key feature will be used on this unit, create an RSA public/private key pair.

e. Enter an initial Network Key. This key may be remotely updated from the Gateway later if the UPuK/UPrK pair has been generated.

f. Configure all network units using steps a through e.

Refer to the Telkonet Gateway user guide and the Telkonet IBMU user guide for detailed description on configuring the Telkonet system.

Section 4 Mitigation of Other Attacks Policy

The module does not claim to mitigate against any other attacks.

Section 5 List of Acronyms

AES `	Advanced Encryption Standard (FIPS Pub197)
ASCII	American Standard Code for Information Exchange
CBC	Cipher Block Chaining
CLI	Command Line Interface
CRC	Cyclic Redundancy Check
FIPS	Federal Information Processing Standard
KAT	Known Answer Test
PLC	Power Line Communications