Telkonet

G3 Series Gateway

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 G3 Series Gateway 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. The Telkonet G3 Series Gateway includes the Gateway, iBridge and eXtender. These components are hardware devices containing firmware. The Coupler is an interface device that contains no security components and is outside the cryptographic boundary.

This document concentrates on the description of the Telkonet Gateway.

1.1 Purpose

The purpose of this security policy is to provide the operator with a specification of the Telkonet G3 Series Gateway and the rules under which the module operates. The model described in this document is concentrated on the Telkonet Gateway.

1.2 Description

The Gateway is enclosed in a metal case, which defines the cryptographic boundary for each unit. The Telkonet Series Gateway is a FIPS 140-2 level-2, multi-chip standalone module. 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 used for key wrapping	
	SHA-256 used to hash the CO password	

1.2.1 Identification

Product name: Telkonet G3 Series Gateway.

Hardware module numbers:

Gateway Models: G3001, G3201 (Firmware version: GAF4.1.0 and GAF4.2.0)

The physical boundary is the casing of the gateway. The cryptographic engine is loaded into FLASH as part of the gateway firmware.

1.2.2 Interfaces

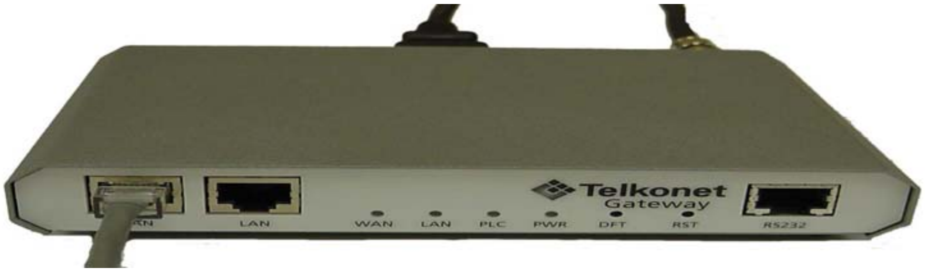
Gateway: Power interface, 100-240 VAC, 0.25 Amps

Power line carrier interface (to coupler): 75 ohm F connector

Carrier frequency. 4 to 21 MHz

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

Command Line Interface: RS-232 Serial, RJ-45 connector.



1.2.3 System Overview and Configuration

The Telkonet solution consists of four devices: the Gateway, the iBridge, the Coupler, and the extender.

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.

Several software applications run on the Gateway to allow for remote management of the system. These include Telnet, Web and SNMP.

The Gateway allows multiple sessions on different management interfaces. Simultaneous status and statistics retrieval does not harm the system. Simultaneous configuration sessions are strongly discouraged although not prohibited.

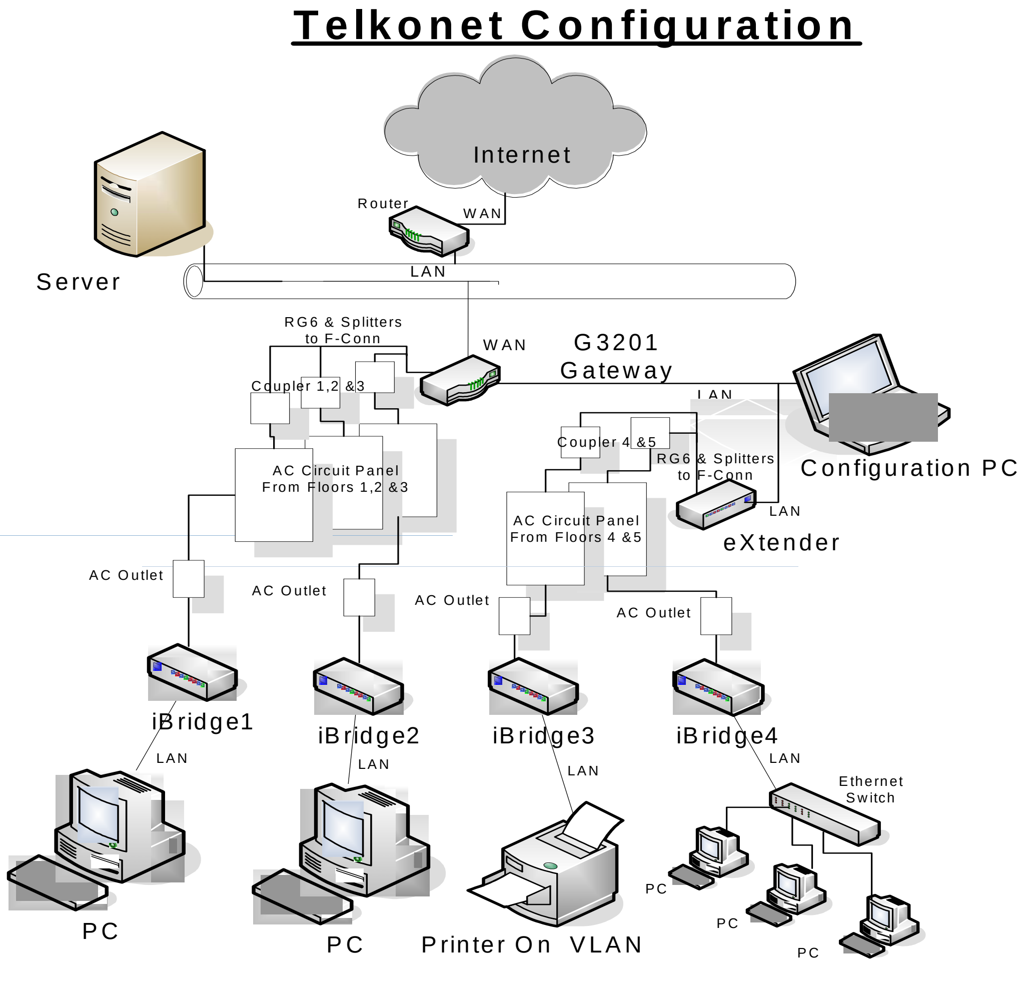


Figure 3

1.3 Scope

The scope of this security policy includes the identification of the Series Gateway, 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 Gateway 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. In the case of the gateway, 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 SHA-256 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 Hashed with SHA-256
User	Role Knowledge of Secret Key	256 bit AES key	2^256

Table 1 Roles

2.1 Telkonet G3 Series Gateway Services

Services provided by the Telkonet G3 Series Gateway 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	Zeroization
User	Encryption
User	Decryption

Table 2 Roles and Services

The Telkonet G3 Series Gateway 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 Hashed with SHA-256	FLASH	W/E
Authentication	User	Secret Key	FLASH	E
Key Entry	C-O	Secret Key	FLASH	W
Key Entry	C-O	Public Key	Gateway FLASH	W
AES Encryption	User	Secret Key	FLASH	E
AES Decryption	User	Secret Key	FLASH	E
RSA Key wrapping	User	Public Key	Gateway 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

Key is generated outside the module and loaded into the Gateway by the crypto-officer using manual methods (i.e. keys are input through the keyboard of the management console that is directly connected to the gateway).

The stored network key is not viewable by the crypto-officer and must be changed at regular intervals. All units in the network must share the same network key.

The network uses an RSA public/private key pair to transport the secret key during re-keying over the network PLC. The Gateway transports the AES NEK to the iBridge/eXtender. Default asymmetric keys are provided and must be changed by the crypto-officer at initial network configuration.

The Crypto-Officer password is hashed using the SHA-256 algorithm.

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 hashed with SHA-256	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 Telkonet Gateway can be reset to factory defaults by manually pressing the reset button and the test button on the Gateway following instructions in the user guide. A factory default operation resets all keys and passwords contained in the module to factory defaults. This will erase the AES secret key and the C-O password as well as iBridge/eXtender public keys stored in the Gateway.

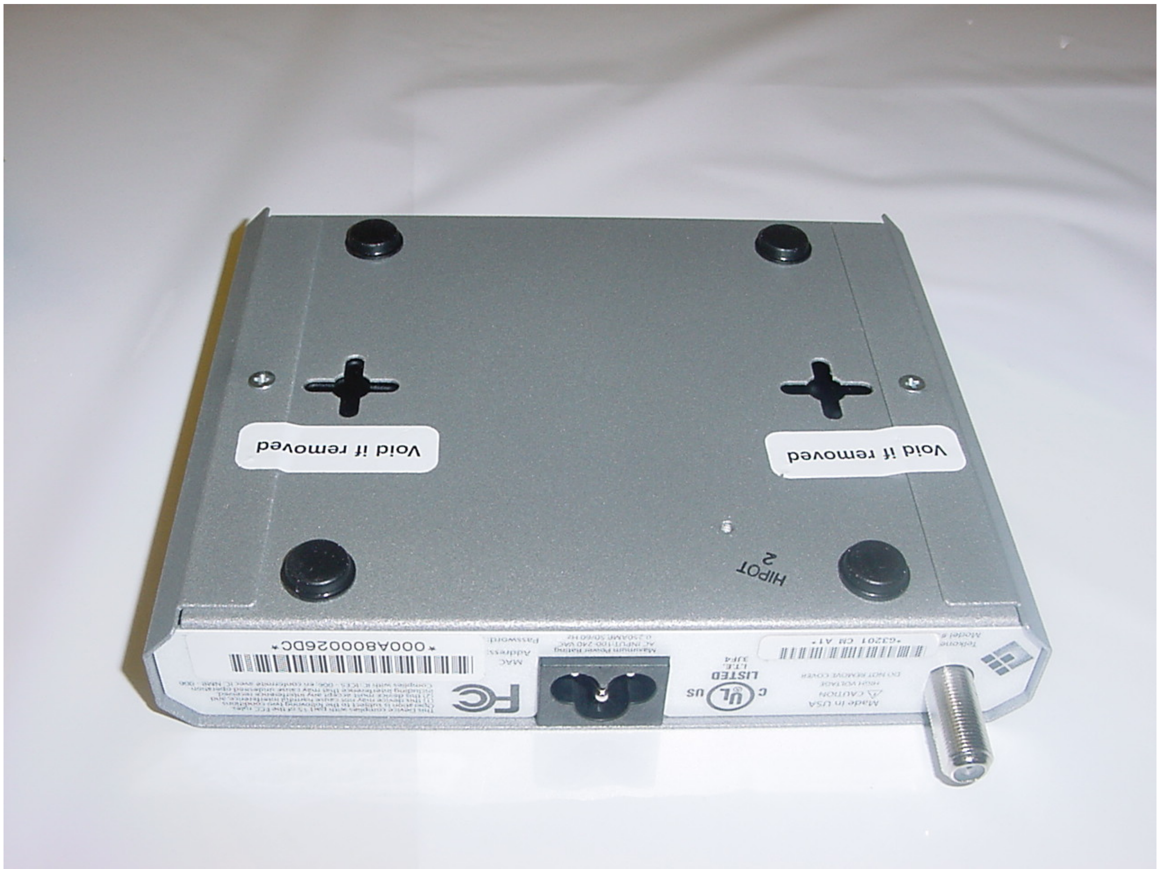
Section 3 Physical Security Policy

3.1 Secure Operation

The Telkonet Gateway is contained within metal cases and protected with a tamper evident seal. Physical access to the Gateway 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 to two seams as shown below: For operational gateways, a label is applied to each seam using the directions given in the Gateway User Manual. This ensures that the cover cannot be removed without tamper evidence being visible. The labels must be applied as specified in the Gateway User Manual.



Telkonet expects the Gateway to be used in a controlled space. Telkonet recommends that the modules be inspected regularly for evidence of tampering according to the following schedule.

Gateway	Weekly

3.1.2 Status Indicators

The Telkonet Gateway shown in section 1.2.2 shows 4 LEDs from the left of the device and two buttons located on the right side of the device. This section describes the function of the LEDs.

3.1.2.1 Gateway LEDs

The module employs LED status indicators to indicate its status and health.

The LEDs are defined to be (from left to right on the front of the box):

1. WAN (WAN Ethernet Link/Activity)
2. LAN (LAN Ethernet Link/Activity)
3. PLC (Power Line Carrier Activity)
4. PWR (Power)

During normal operation the LEDs will display the following behavior:

1.WAN – WAN Ethernet status: off indicates link down, on indicates link established; flashes when there is activity either on the transmit or the receive side

2.LAN – LAN Ethernet status: off indicates link down, on indicates link established; flashes when there is activity either on the transmit or the receive side

3.PLC - PowerLine Carrier status: normally on; flashes when there is activity either on the transmit or the receive side.

4.Power – ON solid

3.1.2.2 Gateway Error Indications

LED	Indicator	Description
PLC LED	Invalid Network Key	PLC LED flashes 3 times (off) and then pauses (on). This pattern is repeated as long as the error condition exists.
PLC LED	Online FW Integrity test failed or AES KAT failed	PLC LED flashes 4 times (off) and then pauses (on). This pattern is repeated until the unit is power-cycled.
PLC LED	Detecting multiple Gateways on the network	Flashes slowly continuously means the Gateway detects more than one Gateway on the network.

All LEDs	Power-up self test	The combination of all 4 LEDs is a code that indicates which part of the boot process the firmware is in. The error codes are specified in the next several sections describing various LED error behaviors for the Gateway, eXtender, and iBridges respectively. If all tests pass, then the LEDs will show normal operation also described in the next several sections.

Table 5 Gateway 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 power cycling the module.

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 initial configuration procedure is described below:

1. Configure the Gateway with the following steps:

    a. Connect to the Gateway using an Ethernet cable to the WAN interface.

b. Login either using Telnet by typing “telnet 192.168.1.254: 2332” or via the Web busing port 8080.

c. The user id is “admin” and there is no password upon initialization.

d. Make sure the unit is in Gateway-bridging mode. This should always be the case as it is the factory default.

e. Change the password of the Gateway using a minimum of 8 characters.

f. Change the Gateway’s management interface IP address to be on the same LAN subnet.

g. Once the management IP is changed, communication is lost. The CO must log in again using the newly assigned IP address.

h. Configure the FIPS secret key by manually entering the key generated using the Telkonet tool “mnek” (a PC utility). This is the Network Encryption Key.

i. Save the configuration.

Note that the Gateway allows multiple concurrent sessions from different interfaces. It is possible to have several Telnet sessions, Web sessions and SNMP sessions at the same time. All of these sessions could be used to perform the same configuration, status and statistics retrieval operations. However, simultaneous configuration from different interfaces are strongly discouraged. The only two configuration commands that are protected are the save configuration and download commands. Once any of these commands is triggered, no other initiation of them would work until the previous one completes. Refer to the Telkonet Gateway User Guide for more detailed description.

2. 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 outside the module using a utility and manually enter the private key.

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.

3. Copy and paste all the public keys into the Gateway's "Add Bulk Data" Web screen to add all the public keys to the Gateway. These are used later for updating the Network Encryption Key.

4. Save configuration on the Gateway.

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

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	Character Redundancy Check
FIPS	Federal Information Processing Standard
KAT	Known Answer Test
PLC	Power Line Communications