eGauge Systems LLC

SECURITY WHITEPAPER

Article ESA-1009D

June 2, 2014

Contents

1 Overview **2**

2 Network Security **3**

2.1 Incoming Connections 3

2.2 Outgoing Connections 3

2.2.1 Proxy-server connection 3

2.2.2 Time-server connection 4

3 HomePlug Security **5**

3.1 EG301x – HomePlug Green PHY 5

3.2 eGauge2 – HomePlug 1.0 5

This document answers commonly asked questions about how the eGauge device is protected from unauthorized access.

1 Overview

The basic philosophy behind eGauge is that the data stored on the device intrinsically belongs to the owner of the device. As such, eGauge Systems LLC is committed to taking all reasonable precautions to ensure the data is only available as intended by the owner.

For installation and user convenience, eGauge devices can be accessed via the Internet by default. Anonymity of the data is ensured since the device does not store any identifying information such as the owner's address or name. The only information stored on the device that could be used for identification purposes is the geographic location ("Settings→Geographic Location"). For privacy- and safety-reasons, this setting defaults to 0 degrees Latitude and 0 degrees Longitude (a position in the Atlantic Ocean). When changing this setting, we recommend setting it to a location near the installation-location of the device, but not so near that the site could be identified. For example, a reasonable approach is to point it to a nearby major intersection, a city center, or similar.

A privacy-enhancing feature provided by eGauge is "Settings→Min. interval for public public usage data". By setting this option to any value other than ”No restriction” it is possible to restrict the resolution of the power consumption (usage) data to the selected resolution (e.g., 3 hours). Full-resolution data will only be available to local users. This feature is deprecated and should instead be replaced with a site-wide password.

For firmware versions 1.00 and further, it is possible to set a site-password (Settings → Access Control). With a site-password, any access to the device will require authentication with a username and password. Devices which have a site-password established are not listed at http://www.egauge.net/devices/.

For ultimate privacy and security, an eGauge device can be configured to not be accessible from the Internet at all. See the section below entitled "Proxy-server connection" how to accomplish this.

The device configuration is protected from unauthorized changes through username/password authentication. By default, the configuration can be changed from the LAN only with username "owner" and password "default".

Multi-user support makes it possible to define additional users. For each user, one of several access-rights modes can be selected including LAN only or remote. When site-wide password protection is enabled, additional levels of security will be available. A user can be restricted to seeing data & settings, data only, or the view whose name is given by the username. This can be used, for example, to restrict a condo owner to see only the energy data for his/her own condo.

2 Network Security

When an eGauge is installed, it is connected to the site's Local Area Network (LAN) via an Ethernet-cable that is connected to a HomePlug adapter (EG301x or eGauge2), or directly to the eGauge main unit (EG30xx). The installation process does not modify or tamper with any firewall products and/or settings that protected the LAN from unauthorized access from the Internet.

2.1 Incoming Connections

The eGauge device listens for incoming connections for the following services:

- Web service (TCP port 80): This provides the normal user interface to access and manage the eGauge device. If desired, this port could be exposed to the Internet through a suitable firewall rule (e.g., a rule which forwards accesses to port 8080 to the eGauge device at port 80).
- SSH service (TCP and UDP port 22): The secure-shell (SSH) service is used for factory-maintenance and -servicing only and is protected by a unique password that is known only to the manufacturer. This port should never be exposed to the Internet.
- mDNS service (UDP port 5353): Provides the multi-cast Domain-Name Service (DNS) which makes it possible to access the device with a name of the form `http://eGaugeNNN.local/`. This should never be exposed to the Internet.

2.2 Outgoing Connections

eGauge has two outgoing connections it maintains:

- Proxy-server connection – using TCP port 8082 – `d.egauge.net`[1]
- Time-server connection – using UDP port 123 – `north-america.pool.ntp.org`[2]

The eGauge will also connect to `egauge.net` on TCP port 80 for firmware upgrades. This connection is not kept open, and is only used when a firmware upgrade is initiated by the user.

2.2.1 Proxy-server connection

When an eGauge device is powered up, it connects to port 8082 of the server defined in the "Proxy-server hostname" setting under "Settings → General Settings". Normally, this is set to d.egauge.net. When connected to this server, the device will be listed as available at `http://egauge.net/devices/`. This connection then makes it possible to access the device from any point on the Internet. In essence, the proxy-server connection is a bridge to the web-service running on eGauge.

It is important to note here that the connection to the proxy-server is completely optional. It is convenient because it makes the eGauge device accessible from the Internet, so power production and consumption can be checked, e.g., when at work or when on travel. Also, the connection enables automatic monitoring of, say, a solar system's performance, such that a solar installer can automatically detect when something is wrong with the solar system.

[1] This server may differ if the eGauge is connected to an alternate proxy server

[2] This server can be changed from Settings → Date Time

If for any reason it is undesirable to maintain the proxy-server connection, “Proxy-server hostname” can be set to “0” (the number zero, without any quotes). Once this setting is saved and the device restarted, it will only be possible to connect to the eGauge device from the LAN. The device will not be visible from the Internet, unless the site’s firewall rules are changed to allow direct access to the device’s web-server.

2.2.2 Time-server connection

eGauge also maintains a connection to the time-server at `north-america.pool.ntp.org`.

This connection is used to automatically maintain the proper time on the device. If eGauge is unable to connect to this service, it will still work properly. The only downside is that the date and time may need to be adjusted manually from time to time via “Settings → Date & Time”. The time server hostname may also be specified on the Date & Time page.

3 HomePlug Security

3.1 EG301x – HomePlug Green PHY

The EG301x uses the HomePlug Green PHY specification and is compatible with HomePlug AV using 128-bit AES encryption. The eGauge and HomePlug AV adapter may be paired using push buttons located on the devices. All HomePlug AV devices, including the EG301x, come with the default encryption key of "HomePlugAV". This key may be set manually through "Settings → HomePlug".

Like HomePlug 1.0, the signal is limited to about 100ft of wiring, and does not extend beyond transformers. However, the new standard communicates traffic in a broader way, increasing the possibility for an outside device to sniff non-broadcast traffic. Pairing the eGauge and HomePlug adapter will result in improved security.

For additional information, please see the HomePlug AV whitepaper provided by the HomePlug PowerLine Alliance at:

http://www.homeplug.org/tech/whitepapers/HPAV-White-Paper_050818.pdf

3.2 eGauge2 – HomePlug 1.0

The eGauge2 device uses a HomePlug 1.0-compatible link to transmit data to the installation site's LAN. The data on this link is encrypted with 56-bit Data Encryption Standard (DES). For simplicity, HomePlug devices, including eGauge2, ship with a default encryption key of "HomePlug". This key can be changed on the eGauge device either through "Settings→HomePlug" (this feature is available starting with v0.82 of the firmware) or through a HomePlug setup-utility:

http://egauge.net/support/HPE100T_Utility.exe (hosted on egauge.net)

Even without changing the encryption-key, HomePlug data is fairly secure for two reasons:

1. The HomePlug signal's reach is limited to about 100ft of wiring and does not extend beyond transformers. Thus, for most single-family homes, the HomePlug signal will be contained to within the home itself. This is in contrast to a wireless WiFi signal, for example, which usually can be picked up easily outside a home.

2. Even if a neighbor could pick up the HomePlug signal, any traffic other than broadcast traffic is difficult to snoop on because the transmission-characteristics of power-lines is so poor that effectively communication between any pair of devices cannot be picked up by a third device. In other words, the worst that could happen in such a scenario is that the neighbor could pick up some broadcast traffic or could use your Internet connection for their own purposes.

In other words, for best security, we recommend changing the HomePlug encryption password, but even without doing so, most sites likely will be fine. Additional information can be found in a whitepaper provided by the HomePlug PowerLine Alliance:

https://www.homeplug.org/tech/whitepapers/HP_1.0_TechnicalWhitePaper_FINAL.pdf