SECURITY WHITEPAPER

January 5, 2017

Contents

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.

1.1 Personal information

For installation and user convenience, eGauge devices can be accessed via the Internet by default. Accessing a device through the proxy-server is anonymous; the user accessing the device interface cannot trace the IP address where the eGauge resides.

Anonymity of the data can be ensured since the device does not automatically store any identifying information such as the owner's address or name.

Because the eGauge is highly customizable, there are areas in which an owner can store identifying information. Register names are chosen by the party configuring the device, so generic names like "Grid" or "Furnace" will not disclose specific owner details, but a name like "The Smith's living room" may.

Other 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. Other options in preferences, such as "Approximate location expressed as a ZIP/Postal code" or "Custom device name to use in web-page titles" could be used to store identifying information.

It is up to the device's owner to decide how much personally identifying information the eGauge device stores and whether to password protect the data (see following section).

1.2 Password protection

On 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). The proxy service allows this service to be accessed remotely normally without requiring changes to the local network firewall or router.
- 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. **NOTE**: This service has been disabled on eGauge2 and EG30xx starting with firmware v3.02.
- mDNS service (UDP port 5353): Provides the multi-cast Domain-Name Service (mDNS) 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.
- BACnet/IP (UDP port 47808): If enabled, eGauge will listen for BACnet connections on UDP port 47808. Default settings are to disable the BACnet server.
- UDP data transfer (UDP port 59046): Proprietary protocol for data exchange when using a remote device as "remote eGauge via UDP".
- HTTPS (TCP port 443): Later generation EG30xx devices will listen for secure HTTP connections on port 443. This service is not supported at this time but can allow for secured communication.

2.2 Outgoing Connections

eGauge has two outgoing connections it maintains:

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

The eGauge will also connect to `egauge.net` on TCP port 80 for firmware upgrades and fetching available data sharing providers when the settings menu is opened (listed in "Settings → Data Sharing"). This connection is not kept open, and is only used when a firmware upgrade is initiated or the Settings page is opened by the user.

[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

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.

Access via the eGauge proxy server keeps the device location anonymous. The public IP address the eGauge is connected from is unavailable to the user accessing the device interface via the proxy server. All data transfered between the user and device is handled by the proxy server, never allowing the user to talk directly to the device. This only applies when connecting remotely over the eGauge proxy server.

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.

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. Disabling the proxy server connection will remove the ability for eGauge staff to perform advanced troubleshooting on devices, and data collected by eGuard will be unavailable.

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.

2.3 Device hostname and network settings

A static IPv4 address may be configured in "Settings → Network settings". The hostname may also be changed here.

The device hostname is used to authenticate the eGauge when connecting to the proxy server. If the hostname is changed without prior notification to eGauge support, the device will not connect to the proxy server. If a hostname change is desired, please contact eGauge support at support@egauge.net before doing so.

3 HomePlug Security

Additional information can be found in the HomePlug Alliance Website at http://www.homeplug.org/.

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.

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:

https://egauge.net/misc/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.