Application Note

SignalFire Wireless Security

OVERVIEW

As the use of wireless technology for sensor and control systems is becoming more and more common, the need for strong wireless security is a requirement. SignalFire has implemented a suite of security features to provide both a reliable and secure wireless network infrastructure.

The security feature has been designed to be as simple as possible for the installer to enable and maintain, while still providing the strong security needed. Using the SignalFire ToolKit software, a "key" is entered in the gateway and each remote node. The key is internally converted in the firmware to the AES encryption key to be used to secure all communications. The encryption key is never sent over the air. Optionally the key can be set to be unrecoverable, so that once it is set it can never be read back out even with physical access to the device.

SECURITY DETAILS

Encryption Standard

SignalFire has chosen the Advanced Encryption Standard (AES) as specified by the U.S. National Institute of Standards and Technology (NIST). A 128bit key size, commonly known as AES128, is used. This encryption standard is used by the US government, financial institutions, banks, and e-commerce sites.

Data Integrity

In any wireless system it is necessary to ensure that all data passed is valid and has not been tampered with in any way. This prevents a malicious attacker from intercepting a packet and intentionally changing its contents. If data is used without an integrity check, unknown actions can occur. A CBC-MAC algorithm using AES128 is used on the encrypted payload data to generate an authentication code (MAC) that is sent along with the data. If any of the data is modified, the authentication code will no longer be valid and the data will be ignored.

Device Authentication

For a node to join the network it must first pass an authentication check. The device authentication messages are encrypted and an encrypted one-time-use token along with address information is passed from the node to the network it is attempting to join. The token is decrypted by the Gateway (or other joined node) using the network key, and if it passes the integrity check and decryption it will respond with a packet containing the token, address information, and network time. The use of the token prevents a rogue network from attempting to absorb joining nodes, preventing them from communication with their intended network.

Replay Prevention

A common security attack is one where a packet is captured and simply re-transmitted at another time. For example, a message to turn on a relay could be captured and then sent again at a later time. Without replay prevention this message could be resent and the receiving node would not know that this message is from an attacker. Many wireless encryption standards do not protect against this type of attack.

SignalFire has implemented a replay prevention scheme based on time synchronization of all nodes in the network. The Gateway generates a time base that is securely distributed to all nodes in the network. Every message received by the Gateway or any node contains the time it was sent. The receiver checks that the time in the message is within a valid receive time window – if it is an old message and outside the window, it is ignored.

Frequency Hopping and Proprietary Protocol

The SignalFire wireless system utilizes a frequency hopping spread spectrum (FHSS) protocol, which means that the RF frequency of transmissions/receptions is constantly changing in a random pattern. This is useful for both advoiding RF interference as well as providing a basic level of security. In addition, the messaging protocol and RF hardware is proprietary and unpublished.

Many standards-based wireless communication protocols have readily available sniffer radios or fully developed hacking platforms. This is not so with the SignalFire system.

A proprietary platform provides an additional layer of security verses a published standard communication protocol, as any attacker would have to crack both the security and the underlying communication protocol at both the hardware and software level.

AVAILABILITY

As of August 1, 2016, SignalFire released new firmware that implements these security and encryption features for all products. All devices after this date are shipped with the new firmware feature. Additionally, the ToolKit has been updated to support this new feature. SignalFire's encryption has been designed to allow backward compatibility with existing networks and be simple to enable on all new network installations.

CONCLUSION

SignalFire has implemented industry standard encryption and advanced security measures to provide a high level of data integrity for any critical process. It includes:

- 128 Bit AES Encryption
- Unrecoverable Key Entry
- Device Authentication
- Replay Prevention
- Proprietary Unpublished RF and Data Protocols