Nota de Aplicación

SignalFire Seguridad Inalámbrica

Introducción

Como el uso de tecnología inalámbrica para sensores y sistemas de control es cada vez más común, la necesidad de una seguridad inalámbrica sólida es un requisito. SignalFire ha implementado un conjunto de características de seguridad para proporcionar una infraestructura de red inalámbrica confiable y segura.

La característica de seguridad ha sido diseñada para ser lo más simple posible tal que el instalador la habilite y la mantenga, a la vez que proporciona la solidez de la seguridad. Usando la herramienta de software de SignalFire el ToolKit, se ingresa una "clave" en la puerta de enlace y en cada nodo remoto. La clave se convierte internamente en el firmware como una clave de cifrado AES que se utilizará para proteger todas las comunicaciones. La clave de cifrado nunca se envía por aire. Opcionalmente, la tecla se puede configurar para que no se pueda recuperar, de modo que una vez configurada, nunca se puede volver a leer, incluso con acceso físico al dispositivo.

Detalles de Seguridad

- ***Encriptación Estandard***

SignalFire ha elegido el Estándar de Cifrado Avanzado (AES - Advanced Encryption Standard) según lo especificado por el Instituto Nacional de Estándares y Tecnología (NIST) de EE. UU. Se utiliza un tamaño de clave de 128 bits, comúnmente conocido como AES128. Este estándar de encriptación es utilizado por el gobierno de EE. UU., Instituciones financieras, bancos y sitios de comercio electrónico.

- ***Integridad de los Datos***

En cualquier sistema inalámbrico, es necesario garantizar que todos los datos pasados sean válidos y no hayan sido alterados de ninguna manera. Esto evita que un atacante malicioso intercepte un paquete e intencionalmente cambie su contenido. Si los datos se utilizan sin una verificación de integridad, pueden ocurrir acciones desconocidas. Se utiliza un algoritmo CBC-MAC que utiliza AES128 en los datos cifrados de la carga útil para generar un código de autenticación (MAC) que se envía junto con los datos. Si alguno de los datos se modifica, el código de autenticación ya no será válido y los datos serán ignorados.

- ***Autenticación del Nodo***

Para que un nodo se una a la red, primero debe pasar una verificación de autenticación. Los mensajes de autenticación del dispositivo están encriptados y se pasa un token de uso único encriptado junto con la información de la dirección del nodo a la red a la que intenta unirse. El token es descifrado por el Gateway u otro nodo unido utilizando la clave de red, y si supera la verificación de integridad y el descifrado, responderá con un paquete que contiene el token, la información de la dirección y la hora de la red. El uso del token evita que una red deshonesta intente absorber los nodos de unión, impidiendo que se comuniquen con su red prevista.

- ***Prevención de reproducción***

Un ataque de seguridad común es aquel en el que se captura un paquete y simplemente se retransmite en otro momento. Por ejemplo, un mensaje para activar un relevo podría capturarse y luego enviarse nuevamente más adelante. Sin la prevención de reproducción, este mensaje podría reenviarse y el nodo receptor no sabría que este mensaje proviene de un atacante. Muchos estándares de encriptación inalámbrica no protegen contra este tipo de ataque.

SignalFire ha implementado un esquema de prevención de reproducción basado en la sincronización de tiempo de todos los nodos en la red. El Gateway genera una base de tiempo que se distribuye de forma segura a todos los nodos de la red. Cada mensaje recibido por la puerta de enlace o cualquier nodo contiene la hora en que fue enviado. El receptor verifica que la hora en el mensaje se encuentre dentro de una ventana de tiempo de recepción válida; si se trata de un mensaje antiguo y está fuera de la ventana, se ignora.

- ***Salto de frecuencia y protocolo patentado***

El sistema inalámbrico SignalFire utiliza un protocolo de espectro ensanchado por salto de frecuencia (FHSS), lo que significa que la frecuencia de RF de las transmisiones/recepciones cambia constantemente en un patrón aleatorio. Esto es útil tanto para evitar la interferencia de RF como para proporcionar un nivel básico de seguridad. Además, el protocolo de mensajería y el hardware de RF son propietarios e inéditos.

Muchos protocolos de comunicación inalámbrica basados en estándares permiten que radios sniffer (robo de datos) fácilmente disponibles o plataformas de pirateo completamente desarrolladas tenga acceso a los paquetes. Esto no es así con el sistema SignalFire.

Una plataforma propietaria proporciona una capa adicional de seguridad frente a un protocolo de comunicación estándar publicado, ya que cualquier atacante tendría que descifrar tanto la seguridad como el protocolo de comunicación subyacente tanto a nivel de hardware como de software.

Transmitter Power/Antenna Design

En los Estados Unidos y Canadá, los sistemas de 915 MHz pueden transmitir potencias de hasta 1 vatio y tienen antenas que pueden duplicar ese rango (+6 dB). Mientras que los sistemas de 2.4 GHz pueden operar con los mismos niveles de potencia en los EE. UU. Y Canadá, la mayoría no supera el requisito global de 0.1 vatios. Las restricciones globales a la frecuencia de 2,4 GHz limitan aún más el rendimiento midiendo la potencia radiada; no se permite ninguna ganancia de antena para un sistema de potencia máxima (0,1 vatios) en la mayoría de los países.

Con los parámetros de operación iguales, un sistema de 915 MHz ofrece aproximadamente 2,6 veces el alcance de un sistema de 2,4 GHz. En la mayoría de los casos, el 915MHz admite un rango más largo entre nodos, beneficioso para las redes inalámbricas de control de sensores que cubren grandes áreas geográficas de cientos de millas cuadradas.

DISPONIBILIDAD

A partir del 1 de agosto de 2016, SignalFire lanzó un nuevo firmware que implementa estas características de seguridad y cifrado para todos los productos. Todos los dispositivos posteriores a esta fecha se envían con la nueva función de firmware. Además, el ToolKit se ha actualizado para admitir esta nueva característica. El cifrado de SignalFire ha sido diseñado para permitir la compatibilidad con redes existentes y ser simple de habilitar en todas las instalaciones de red nuevas.

CONCLUSION

SignalFire ha implementado el cifrado estándar de la industria y medidas de seguridad avanzadas para proporcionar un alto nivel de integridad de datos para cualquier proceso crítico que incluyen:

- Encriptación de128 Bit AES (AES128)
- Entrada clave irrecuperable
- Autenticación del dispositivo
- Prevención de reproducción
- Protocolos de datos y RF no publicados patentados