Application Note

SignalFire RANGER MQTT Security

OVERVIEW

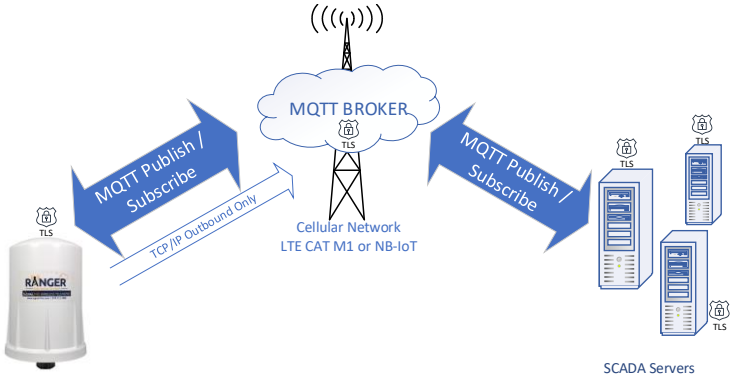
With the increase of wireless technology and Industrial Internet of Things devices (IIoT), security is an important concern. The SignalFire RANGER utilizes the MQTT/Sparkplug protocol, which uses TCP/IP as the transport over LTE-M/NB-IoT cellular networks.

MQTT/Sparkplug does not have a separate security layer; rather it inherits the well proven network security provided by the TCP/IP layer. Even as standards evolve, upgrades to security mechanism make the technology future-proof.

NETWORK TOPOLOGY

The diagram above shows the data flow from the RANGER to a cloud server. First the RANGER establishes a connection to the cellular network, then it opens a TCP/IP connection to the configured MQTT broker. **Direct communication to the RANGER is not possible**, all data passes through the broker.

The MQTT broker acts as a middleman allowing many RANGERs to communicate with one or more servers/hosts in a secure and data efficient manner. Each message from a RANGER is published to the broker where any hosts subscribed to that data will then receive it.



SECURITY DETAILS

Since all TCP/IP connections are initiated by the RANGER to a MQTT broker, the RANGER does not have a static IP address and cannot be accessed directly. The RANGER can't respond to IP inquiries because by design doesn't listen to IP message requests, and all inbound TCP ports are disabled. We recommend that any customers providing their own SIM cards **do not configure them for public IP addresses.**

The RANGER supports TLS 1.2 certificates with full validation; when enabled on both the RANGER and the broker only a secure connection is possible. The RANGER supports 2-way certificate validation providing true end-to-end security without the complexity of VPNs etc.

Once the data is pushed to the MQTT broker, one or more servers can subscribe to that data. Again, the broker can be configured so that it only accepts connections over a TLS secured port.

SIGNALFIRE CLOUD SECURITY

When a RANGER is used with the SignalFire Cloud service, each RANGER is loaded with a set of factory TLS certificates from a Certificate Authority (CA) that allow it to connect to the SignalFire Cloud MQTT broker. The set of TLS public/private certificates are authenticated by the CA before a connection can be established. The MQTT broker is running on an AWS instance along with the SignalFire Cloud Ignition server and database.

User access to the SignalFire Cloud dashboard is provided over a HTTPS connection and is protected by a username and password.

PHYSICAL ACCESS PROTECTION

If someone were to gain physical access to a RANGER, a common concern is that someone could connect to it using the USB port and read and/or change its settings. To prevent against this, the RANGER firmware has an optional password for USB port access. Once the password is enabled, a user can only reset a device to factory defaults unless they have the password, protecting any credentials or settings that may have been configured.

In addition to the USB password, the TLS certificates are write only, meaning they can never be read out of a RANGER.

CONCLUSION

The SignalFire RANGER is designed using proven TLS security standards that are used everyday to secure websites, email, and voice over IP connections. The SignalFire Cloud MQTT broker and server reside on AWS which powers many enterprise websites. Combined they provide a secure end-to-end solution you can count on.