OmniSense FMS Network Security

Anytime you tell your network administrator you plan to plug a wireless gateway into your network the first question they will ask is “Is it “secure”?”. The usual answer talks about 128 bit encryption, passwords and other common forms of security. With these methods of security experienced network administrators understand that total security is not possible but rather the question to ask is “How hard is it to defeat?”. The OmniSense FMS takes a unique approach that simply does not provide any method for wireless access to your network. Perhaps the best way to describe the security of the system is the old saying “You can’t get there from here.” Because wireless access to your network is by design not possible it renders analysis of the strength of encryption or passwords mute.

How Does It Work?

Gateways continuously announce their presence by sending a wireless beacon signal. Sensors wake up and scan for the beacon signal. Once the beacon has been detected the sensor sends a HELLO packet to the gateway announcing its presence. The gateway then reads the sensor’s log file, opens a TCP/IP connection to the OmniSense Database Server (ODS) and sends the log file as XML/HTTP message to the ODS. A sensor can not send any commands to the gateway nor does the gateway support any commands from the wireless interface. There is no “secret back door” that can be exploited. The worst a hacker can do is clone a sensor and send bogus sensor data to the ODS. The Gateway’s TCP connection configuration information can only be modified from a LAN connection and access to the Gateway’s configuration is password protected so it would be difficult but not impossible for a hacker to redirect the data to another TCP/IP destination.