RTLS LPWAN data security

VERSION 1.0 | MARCH 2018 | RTLS

Summary

The RTLS LPWAN tagging system is based on a unique 32bit ID number and other data which is transmitted by Radio Frequency using a *tag* which is fitted to each item, and a *gateway* which receives this data and relays it to the RTLS systems.

In principle no client data is sent within the tag, only within the backend system is the unique 32bit ID associated with any situational data. Therefore, even if data is intercepted, it would only reveal the 32bit number and other activity data from the tag such as temperature, movement and only sets which have little relevance.

Radio Frequency Operation

- all tags transmit on the same frequency within the 868MHz ISM band, for a brief period of time (mS), the frequency of transmission is not in the public domain. It is difficult to obtain this frequency of operation in the field without specialist equipment, knowledge and time to accumulate and average signal over hundreds of transmissions. Even in that circumstance one would need prior knowledge of the band and channel in comparison to all the existing transmissions and other device usage in the same band to make an association.

- data can only be read by one specific device hardware type unless complex specialist technology is employed, again this would require prior knowledge of the hardware type. It is extremely difficult to determine in a field operation.

- once that frequency and hardware type is known, a specific hardware key is utilised to prevent cross reading of other applications using that same hardware type in the field. This is a secret key within the firmware of the hardware device. In addition, other hardware settings such as data length, CRC and other configuration types which are also only found in the firmware of the device would have to be obtained.

- if all of this is known, the data transmitted is scrambled before transmission using methodology again only within the firmware. Again, this would require inside knowledge, or direct access to the device hardware.

- the data packet size and protocol are not in the public domain, so any data intercepted to this level would also require knowledge of the protocol to identify data of interest.

- as stated above, if the system is compromised the outcome would still require knowledge of the relationship between the unique 32bit number and any client data, meaning both the hardware and backend systems would have to be compromised to identify any assets of interest.

Gateway

- the gateway collects the tag IDs and sends encrypted data to the server via https. Even if a third party decrypts the data, they will have to know what asset is associated to the tag ID to know the contents of the transport.

Portal

- all data is accessed via a secure https connection. The data-base in use at RTLS is an SQL Server hosted on Microsoft Azure. The system (STRAQ) has been tested in the past by PwC and passed their WASA (web application security assessment).

- as an alternative, the client could host the system on their own servers.

Version 1.0 March 2018