BARDIC

Whitepaper

BARDIC Emergency Lighting

How secure is a centrally monitored emergency lighting system?

Introduction

The main egress routes from a building or high risk areas must be sufficiently lit in case of a power failure. The emergency lighting systems are therefore subject to strict guidelines that must comply with the Building Code of Australia and the relevant Australian Standards (AS2293). Inspection and maintenance of exits and emergencies are often a high cost due to the stringent requirements of the Australian Standards. Centrally monitored systems are one solution to that problem that provide easy and cost effective monitoring, control, and management of emergency fittings. Most of these systems rely on communication wires/cables that interconnect each of the emergency fittings to a central device. This however, introduces additional complexities in terms of installation.

The BARDIC Solution

BARDIC provides a solution that does away with the physical wired interconnection and the potential problems associated with it. The WINET RF™ is a self-healing, wireless mesh network system that offers building owners, maintenance managers or service agent's total control over their assets and public safety obligations, and helps manage installation and the maintenance of an emergency lighting system. More often than not, consumers immediately question the network security of the system at the very mention of wireless.

Wireless Not Necessarily Wi-Fi

Firstly, clarification is necessary as consumers often mistakenly assume that the term wireless immediately refers to Wi-Fi (IEEE 802.11). However, this is not the case for the Wi Net RF™ as it is based on the ZigBee standard (IEEE 802.15.4). The radio band (920 MHz) used by the Wi Net RF™ is completely separate to that of Wi-Fi networks (2.4GHz and 5GHz) thus, provide no interoperability.

Network Security

The term network security must first be defined and understood in order to answer the question of how secure the WINET RF™ is. First and foremost, take note that no network is perfectly secure and one is only as secure as its weakest or least secured component/device/access point.

In this context, consumers are most concerned with the WINET RF™ acting as a relatively easy gateway or back-door into their local computer network, bypassing any security measures that may have been employed. This would allow an attacker unauthorised access to the network thus, compromising private and sensitive data on the network or even the integrity of the network itself. Less frequently, consumers are also concerned with the security of the WINET RF™ system itself as it forms its own wireless mesh network for inter-node communication. The risk here is a malicious entity (an individual or a body/organization) may gain access to the emergency lighting system.

ZigBee Wireless Mesh Network

The latter security risk will be addressed first as it is fairly straightforward. It is public knowledge that the WINET RF™ employs ZigBee transceivers and operates on 920 MHz with O-QPSK (offset quadrature phase-shift keying) modulation. Beyond that, communications between nodes are encrypted with a 128-bit AES (Advanced Encryption Standard) secret key which is known only to the BARDIC. The encryption/decryption is performed in hardware and is identical to that employed by the IEEE 802.11i, better known as WPA2 (Wi-Fi Protected Access II) for Wi-Fi networks. The general public would recognise WPA2 as one of several available security measures that prevents unauthorised connection to a wireless router. A brute force search for the secret key is unfeasible as it would take years with current technology. An easier alternative would be to simply acquire a physical copy of the WINET RF™ node module and reverse engineer the communication protocols however, this falls into the realm of physical security.

Assuming that a malicious entity, against all odds, gained access to the WINET RF™ mesh network, the potential damage that can be caused for the most part can be dismissed as mere nuisances. The primary task of the WINET RF™ is to initiate discharge tests of the batteries in an emergency fitting. The switching of the emergency fitting to operate on mains or battery power is the one and only active action that is possible given the physical circuit design of the node module. Given that, a malicious entity could intentionally attempt to fully discharge the batteries of an emergency fitting, leaving the emergency fitting with no backup power in the event that the mains power fails before the batteries recharge. However, this is improbable unless the malicious entity completely re-programs the system as there are algorithms in place

"One major misconception involves assuming that because the WINET RF™ platform is wireless it operates on a standard Wi-Fi connection. In fact, the opposite is true".

prevents the batteries from fully discharging. Additionally, the switching to and from battery power triggers a visible (and sometimes audible) change in the emergency fitting which, may not get by unnoticed. In the unlikely event that the batteries are fully discharged, normal operation would resume after the batteries are recharged. Apart from this worst case scenario, a malicious entity gains access to information on the emergency fitting (battery voltage, light status, etc.) which, by itself can cause little to no direct harm.

Local Area Computer Network

Moving on to the more serious issue of computer network security, the WINET RF™ system requires that one or more SMARCO (SMart ARea COntroller) devices to be connected to the local area network. This is viewed as a potential entry point for attackers as all nodes communicate back to a SMARCO. As mentioned previously, communication between nodes are encrypted and breaking the encryption implies that an attacker would also gain access to a SMARCO (also considered a node) that is connected to the local area network. However, a SMARCO plays a much more active role than a regular node in the mesh network. Commands can only be issued by a SMARCO while regular nodes are only able to accept commands or relay them to another node. A SMARCO can accept responses from nodes but it is not programmed to respond to commands. Additionally, the communication protocol used in the mesh network is simplistic yet strict. Communication messages consist of well-defined key-value pairs whereby unknown keys are simply discarded while all values are precisely bound. All this means that an attacker coming in from the ZigBee wireless mesh network are severely limited by what then can perform and access on the local area network.

A more likely point of entry is via the web-based GUI (graphical user interface) hosted by the SMARCO on the local area network. However, this implies that the attacker would have already had access to the local area network, or a subset of it, and can just as easily exploit any other available services or devices. An attacker may also gain physical access to a SMARCO which can be exploited to access the local area network. Again however, this is an issue of physical security and a SMARCO should not have been physically accessible to unauthorised personnel to begin with.

Summary

To summarise, the WINET RF™ operates at a different radio frequency compared to Wi-Fi networks thus provide no interoperability. AES encryption is also employed for communication between nodes to prevent intercepts. Gaining control and access to the WINET RF™ wireless mesh network at best would allow a malicious entity to fully discharge the batteries and even before that, they would have to bypass algorithms that prevent such an action. A malicious entity would also gain harmless information (battery voltage, light status, etc.) regarding emergency fittings in the network. Attacks targeting the local are computer network originating from the WINET RF™ wireless network are virtually impossible as communications between nodes and SMARCOs are predominantly one-way. SMARCOs accept only response messages from nodes while nodes are incapable of issuing commands. All these features ensure that the security of the local area computer network is not compromised whatsoever by the fact that the mesh network of the WINET RF™ is wireless. WINET RF™ is as secure as, if not more than, the majority of common network attached devices currently available.