Chapter 1

Security Threats and Risks of Intelligent Building Systems: Protecting Facilities from Current and Emerging Vulnerabilities

David Brooks
Edith Cowan University, Australia

ABSTRACT

Intelligent Buildings (IB) are facility-wide systems that connect, control, and monitor the plant and equipment of a facility. The aim of IB is to ensure a facility is more efficient, productive, and safe, at a reduced cost. A typical IB integrates diverse subsystems into a common and open data communication network, using both software and hardware; however, IBs suffer from diverse generic vulnerabilities. Identified vulnerabilities may include limited awareness of security threats and system vulnerabilities, physical access to parts of the system, compromise of various networks, insertion of foreign devices, lack of physical security, and reliance on utility power. IB risks are contextual and aligned with the threat exposure of the facility. Nevertheless, there are generic mitigation strategies that can be put in place to protect IB systems. Strategies include threat-driven security risk management, an understanding of system criticality, greater integration of departments, network isolation, layered protection measures, and increased security awareness.

INTRODUCTION

Intelligent Buildings (IB) or Building Management Systems (BMS) are building-wide control systems that connect, control and monitor the fixed plant and equipment of a facility. Increasingly into the future, such systems will be installed and operated in many building types, from Critical Infrastructure facilities to residential buildings. These systems allow the facility users to have a much better experience. For example, when a person first arrives at work in the morning and uses their RFID tag to enter the building, the IB system will call the lift to the foyer, allow access to their designated floor, and their office lights and Heating, Ventilation and Air-Conditioning (HVAC) will turn-on. The IB system keeps the lights and HVAC operating while it detects move-
ment in their office and the adjacent area, turning these off when that person leaves for the day.

While there is no single definition for IBs, the following one summarises elements commonly associated with IBs:

A system that supports the flow of information throughout the building, offering advanced services of business automation and telecommunications, allowing furthermore automatic control, monitoring management and maintenance of the different subsystems or services of the building in an optimum and integrated way, local and/or remote, and designed with sufficient flexibility to make possible in a simple and economical way the implementation of future systems (Lafontaine, 1999).

IBs integrate and enable connectivity within the plant and equipment subsystems of a facility, including security systems. In the last ten years or so, IBs have become a significant factor in the design, build, operation and maintenance of commercial buildings. Such systems have become popular due to the need to save energy, provide more reactive and safer facilities, and reduce operational costs. Many of these facilities contain classified material or critical assets. As SCADA system vulnerabilities have been exposed, IBs suffer similar vulnerabilities. Whether the system is an IB or SCADA system, both may control and monitor Critical Infrastructure.

The ability of IBs to integrate diverse subsystems is achieved through common and open data communication protocols and hardware. Such an open approach leaves facilities vulnerable to both external and internal threats and risks. Depending on the threat environment of a facility, vulnerabilities can be diverse and occur throughout many parts of the IB such as vulnerable hardware devices, insecure software and various insecure networks. From a security perspective, IBs are still at an early stage of understanding and the feasibility of such technological solutions should be considered from the onset, as privacy, information control and security are often neglected (Gadzheva, 2008, p. 6).

Many of these systems are designed and installed by building engineers, and owned and operated by facility managers, with both groups generally having limited security awareness.

IB vulnerabilities cover a broad range of potentially exploitable systems. These vulnerabilities open up many approaches for using IB systems for covert or illegal activities. Being able to log into most parts of an IB system, in particular, the automation network level will allow a “picture” of the facility to be built up. For example, when a person first arrives at work in the morning and uses their RFID tag to enter the building, this is communicated throughout the IB System. It is possible to then track that person as various systems turn on or off triggered by various room sensors. When the CEO is in their office and as they leave, it becomes a relatively easy monitoring task to track their movements. When and where security guards patrol the facility and their current location after hours can also be tracked. Finally as security devices such as detectors and CCTV are incorporated into IBs, this allows these devices to be turned off for a period of time to allow illegal access.

Therefore, the objectives of this chapter are to provide:

- An overview of Intelligent Building systems and their architecture, both software and hardware.
- Present generic Intelligent Building systems vulnerabilities.
- Provide generic mitigation strategies to protect Intelligent Building systems.
- Raise awareness of Intelligent Building systems vulnerabilities and the need for directed mitigation strategies.

**BACKGROUND**

Intelligent Buildings (IB) are becoming increasingly popular, driven through the need to save
Related Content

Germany's External Trade Development: A Case of the German Automotive Industry
www.igi-global.com/chapter/germanys-external-trade-development/171839?camid=4v1a

Disaster Management and Continuity Planning in Libraries: Literature Review
www.igi-global.com/article/disaster-management-and-continuity-planning-in-libraries/148212?camid=4v1a

Firewalls as Continuing Solutions for Network Security
www.igi-global.com/chapter/firewalls-continuing-solutions-network-security/20643?camid=4v1a

Risk Planning with Discrete Distribution Analysis Applied to Petroleum Spills
www.igi-global.com/article/risk-planning-with-discrete-distribution-analysis-applied-to-petroleum-spills/106030?camid=4v1a