Edith Cowan University
Research Online

Australian Security and Intelligence Conference | Security Research Institute Conferences

2011

Intelligent buildings: an investigation into current and emerging security vulnerabilities in automated building systems using an applied defeat methodology

David J. Brooks
Edith Cowan University

Originally published in the Proceedings of the 4th Australian Security and Intelligence Conference, Edith Cowan University, Perth Western Australia, 5th -7th December, 2011
This Conference Proceeding is posted at Research Online.
http://ro.ecu.edu.au/asi/11

INTELLIGENT BUILDINGS: AN INVESTIGATION INTO CURRENT AND EMERGING SECURITY VULNERABILITIES IN AUTOMATED BUILDING SYSTEMS USING AN APPLIED DEFEAT METHODOLOGY

David J Brooks
secau Security Research Centre, School of Computer and Security Science
Edith Cowan University, Perth, Western Australia
d.brooks@ecu.edu.au

Abstract

Intelligent Buildings (IB) have become increasing popular during the past decade, driven through the need to reduce energy, have more reactive and safer buildings, and increase productivity. IB integrate many systems that were in the past isolated from each other, including fire and life safety, HVAC, lighting, security, etc. Facilities contain commercial-in-confidence material and other valued assets; however, IB are integrated through open and common data communication protocols and hardware, leaving facilities exposed to external and internal threats. The study presents an investigation into IB, based on a defeat evaluation methdology.

IB vulnerabilities considered two areas, namely physical and software vulnerabilties. Physical hardware vulnerabilities included physical access to the automation devices or workstations, communication networks, wiretapping, remote connectivity, foreign devices and local field programming. Software vulnerabilities included common connectivity protocols, restricted encryption and limited security considerations. These vulnerabilities could result in such attacks as denial of service, covert facilty entry or espionage. IB risks are contextual, aligned with the facility's threat exposure; nevertheless, there are generic mitigation strategies that can be taken to protect IB systems. Protection includes situational threat driven security risk management, understanding system criticalities, integration of departments, a degree of network isolation and greater awareness.

Keywords

Intelligent Buildings; Building Management System; vulnerabilities; mitigation

INTRODUCTION

Intelligent Buildings (IB) or Building Management Systems (BMS) are building wide control systems that connect, control and monitor a facility's system, subsystems, and plant and equipment. There is no single definition for IB's, although the Institute defons Cerdá suggest that they are a:

> "system that support 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." (cited in Lafontaine, 1999)

IB's integrate and enable connectivity within the majority of a building's plant and equipment systems, including security systems. In the last decade or so, IB's have become a significant factor in the design, build, operation and maintenance of commercial buildings. Such systems have become increasing popular, driven through the need to save energy, provide more reactive and safer facilities, and reduce operational costs.

IB technology is incorporated into many facilities, some which contain classified material, premises and other assets. These classified protected areas contain many systems, such as fire and life safety, etc., with broader incorporation and integration into traditional electronic, electrical, mechanical and pneumatic systems. Nevertheless IB's are still at an early stage, but 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). These systems are integrated through common and open data communication protocols and hardware that leave facilities vulnerable to both external and internal threats and risks.

Study objectives

The objectives of the study were to investigate Intelligent Building (IB) systems and their architecture, both software and hardware. The investigation used an emulated bench-mounted IB system to evaluate vulnerabilities from which mitigation strategies could be put forward.

WHAT ARE INTELLIGENT BUILDINGS

In the last two decades integrated Intelligent Buildings (IB) systems have become a significant factor in the design and build of commercial buildings. There is also a trend to retrofit existing buildings in increasing numbers, where cost returns to stakeholders are positive. For example, the Empire State building installed an integrated IB with the aim of reducing energy use by 40% (Schneider & Rode, 2010). IB's are primarily about creating operational efficiency and effectiveness of the multiple and disparate systems that make up a modern commercial building. Such systems may include standard and emergency lighting, fire and life safety systems, heating, ventilation and air-conditioning (Figure 1), emergency warning and intercommunication (EWIS), elevators and communications. The list of the building components being integrated is extensive and growing, including all security systems.

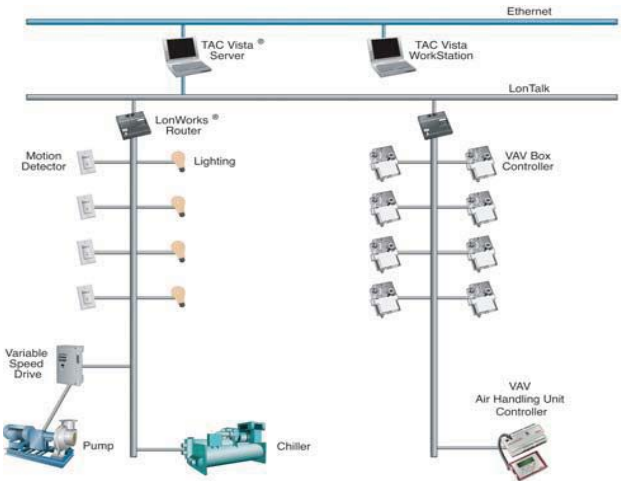

Figure 1. Typical Intelligent Buildings system

(Schneider Electric TAC, 2004, p. 8)

Modern IB's have received widespread acceptance in the commercial property marketplace and are generically defined as a "computer-based control building automation systems predominate in most commercial and industrial buildings, reducing energy costs while improving system performance, operability and reliability" (Langston & Lauge-Kristensen, 2002). Nevertheless, IB's may also be known by several different names including building management system, smart building, building automation system, high-performance building and energy efficient building.

ARCHITECTURE OF INTELLIGENT BUILDING SYSTEMS

A typical Intelligent Building (IB) integrates many component parts onto common networks, using both software and hardware architecture. The European Committee for Standardization (CEN) divides IB communications into three distinct layers, namely *management level*, *automation level* and *field level* (Figure 2).

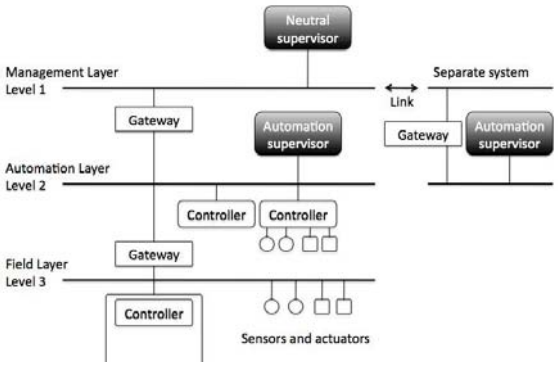

Figure 2. Three layered IB architecture

(CIBSE, 2000)

Hardware Architecture

As Figure 2 demonstrates, an IB system is divided into these three levels of architecture. The management level contains the human interface (workstations), server and routing devices, all connected via an Ethernet communication LAN/WAN using TCP/IP/BACnet. The automation level provides the various primary control and secondary room automation, connected via networked Controllers using twisted-pair cables and operating BACnet, LonWorks or KNX, to name a few. The automation level Controllers provide interface between the IB's upper and lower levels, and contains some distributed intelligence. Controllers are typically designed to either provide specific application functionality or generic functionality, although most still contain some degree of multi-functionality.

Finally, field level devices are connected and operate specific plant and equipment sensor or activators operating such protocols as Modbus or their own proprietary protocol. Field devices are the elements that connect the IB to its physical environment, providing the system with information and the means to continually adjust building environment and safety conditions. There are no single approach to IB hardware application, as the integration of IB devices will depend on the facility's requirements and complexity (Figure 3).

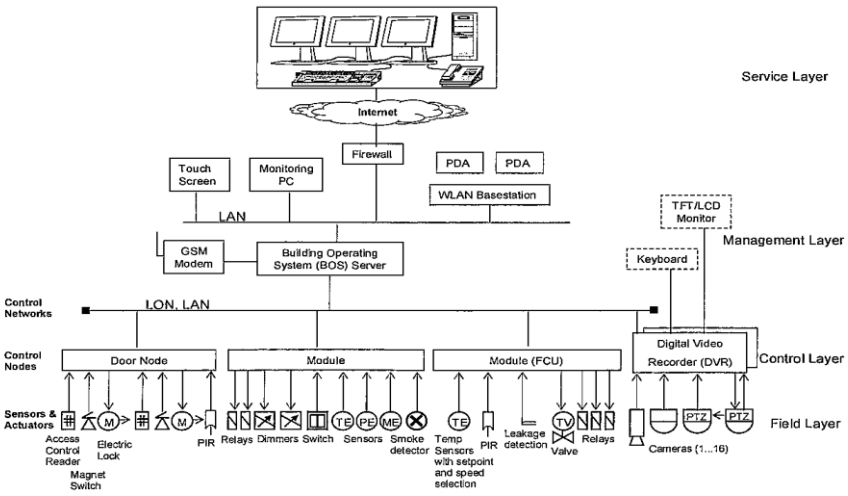

Figure 3. Typical IB system

(Lonix Building Connectivity, n.d., p. 26)

Software Architecture

The management device level primarily consist of a software package that allows human system integration, in general operating on standard software such as Microsoft Windows 2000/XP/2003 with WAN/LAN communication on Ethernet, TCP/IP or other standard network equipment. The software system primarily allows human interface to control, adjust and monitor the facility. Many of the manufacturers provide such software

packages in various modules, allowing users to select what most suits their building and future upgrades. The second level of an integrated IB system is the automation level.

For IB's to function there is a requirement for some form of network that links and integrates the many discrete components. The network needs to be "real-time and have a simple device interfaces comparable with the cheap nature of existing building devices such as light switches" (Sharples, Callaghan, & Clarke, 1999, p. 136). Such a requirement has led to a number of IB network standards and protocols (Table 1).

Table 1. IB industry standards and protocols

Standards or Protocols		
BACnet	Dynet	Modbus
C-Bus	Energy Star	oBIX
CIBSE	EnOcean	OpenTherm
DALI	KNX	ZigBee
DSI	LonTalk	
Midac	OpenWebNet	

(Adjusted from Sharples, et al., 1999, p. 136)

No particular standard for all current IB devices exists nowadays, although the two protocols BACnet and LonWorks have been widely accepted and used as international de-facto standards. Furthermore, the industry has embraced Ethernet connectivity to all IB devices, whether they are primary network or sub-network devices. Connectivity encompasses Direct Digital Controllers (DDC) along with open protocols such as BACnet, LonWorks and Modbus (Figure 4). Contemporary control supports all these protocols, while providing universal input/output connections to temperature sensors, damper actuators, life safety and lighting devices (Automated Buildings.com, n.d.).

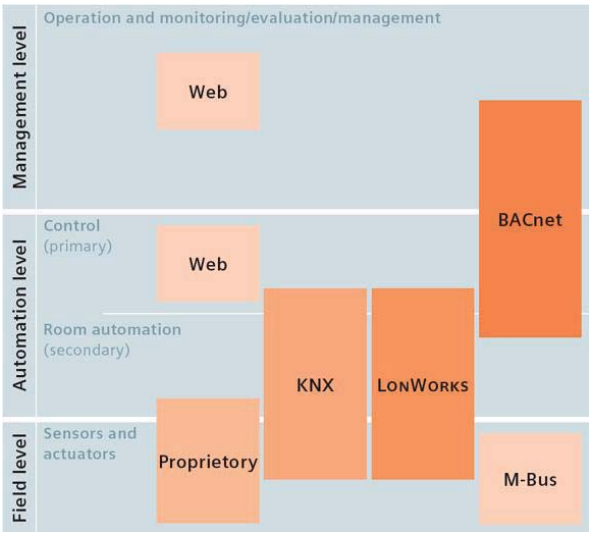

Figure 4. IB software architecture

(Siemens, n.d.)

INTELLIGENT BUILDING VULNERABILITIES

Intelligent Building (IB) systems are exposed to diverse vulnerabilities, such as a facility wide common and open data communication protocols and hardware, and restricted awareness or consideration of security issues. These issues leave IB vulnerable to both external and internal threats. The initial part of the study puts forward a proposed list of *desk-top* assessed vulnerabilities, which informed the defeat evaluation planning.

The intent of IB is to connect and integrate plant and equipment, allowing local and/or remote control and monitoring; however, many of these systems are designed, installed and operated by service engineers, with

restricted consideration of security. The service focus is to maintain the facility's environmental and operational capability, rather than protect the various IB parts beyond locking plant rooms or enclosures. For example, today a Chiller will have the functionality to interface not only to its propriety HVAC system, but also a generic IB system.

IB's are expanded IT networks that are required throughout and into almost every part of the facility, such as plant rooms, service areas, ceiling spaces, etc. In addition, many IB use the IT network as its primary data network. At each component location there will be a Controller, which has all the functionality of a desk computer excluding the user interface. However, there is functionality that allows programming devices to be plugged into the Controller, giving access to the greater IB system and in some instances, the greater IT network.

There has been limited consideration of the vulnerability of IB systems (Gadzheva, 2008), either from such bodies as the International Organizations for Standards (ISO), the IB manufactures, integrators or maintainers. Their focus is to ensure that the many pieces of a facility's plant and equipment integrate and effectively communicate, with little additional interfacing required. Underlying program coding and interface hardware is freely available.

IB suffer from generic vulnerabilities, with the primary difference being the contextual application and therefore, threat to the IB and greater facility. An initial review of likely vulnerabilities ranged from physical access to devices to not having any form of uninterrupted power supply to maintain capability (Table 2).

Table 2. Overview of proposed vulnerabilities

Desk-top evaluation	Vulnerabilities
Device access (physical)	Access & compromise of the Management software
	Access & compromise of the Automation level
Network access (physical)	Access & compromise of the Ethernet
	Access & compromise of the Automation level
	Known unauthorised secret key
	Unauthorised key – loss of integrity
Wiretapping	Access & compromise of the Ethernet
	Access & compromise of the Automation level
EM attack	Wiretap & compromise of the Ethernet
	Wiretap & compromise of the Automation level
Workstation	Access & compromise of the Management software
Remote workstation	Ethernet access with a foreign computer
Foreign device	Automation level insertion of a foreign Controller
Internal & external memory	Extraction of past and insertion of system memory
Device program	Use of an External Programmer at a Controller
Embedded function	Illegal use of embedded functions
Enclosures	Existing enclosure are only dust covers
Anti-tamper	No anti-tamper capability
Power supplies	Whole of system shutdown on loss of power

These reviewed IB vulnerabilities were then used as a priori assessment to develop and plan the evaluation methodology on the emulated IB system.

METHODOLOGY

The evaluation methodology applied a priori evaluation approach, which considered reliability, validity and testing scope (Brooks, 2010). These three aspects were considered to be core principles during evaluation (Jones & Smith, 2005; Smith, 2007) as *reliability* ensures that evaluation is conducted in such a way that results are repeatable, given the same variables and environmental conditions. *Validity* ensures that the evaluation is based on a careful selection and isolated independent variables, and the methodology evaluates what it asset to measure. The *testing scope* included simple to complex physical and technological attacks, resulting in an understanding of the IB's vulnerabilities. A number of discrete steps were taken within the evaluation methodology (Figure 5), commencing with documenting a defined approach to evaluation that ensured a priori testing criteria.

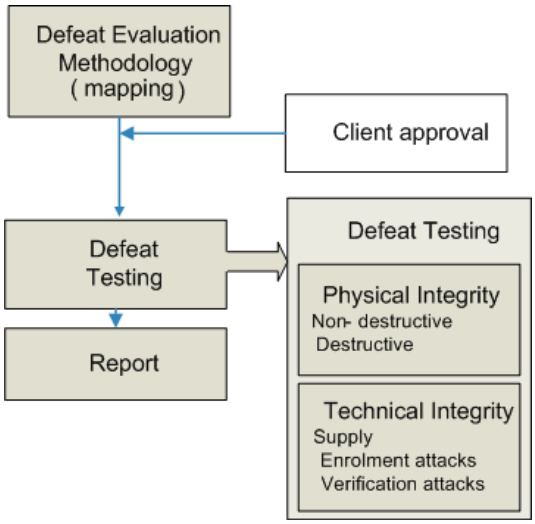

Figure 5. Defeat evaluation methodology

(Adjusted from Brooks, 2010)

An IB system was selected for vulnerability evaluation, based on a number of parameters such as:

1. The system is produced by a international manufacturer within the IB market.
2. Supplier has offices for the design, installation, maintenance and support in most major centres in Australia, and carries a broad range of IB products from the management to device level.
3. The system is used extensively in major facilities around Australia.
4. That the sponsoring agency supported the selection of this system.

The procured system comprised of a number of discrete devices (Figure 6) that were integrated to reflect what could be considered a typical facility IB, although in a smaller scale. The Management level computer was an IBM Laptop, operating a Pentium 1.7GHz with 1GB RAM and Microsoft Windows XP Professional V2002. The IB devices were desk-top mounted onto a board and connected (Figure 6). 7Connections included 240VAC primary supply, data network Ethernet and automation RS-485 BACnet. In addition, a custom manufactured Test Module (Figure 8) was connected to increase the number of inputs (x4) and outputs (x4).

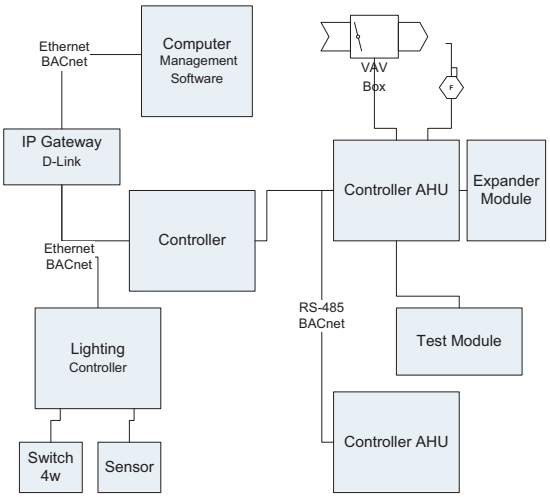

Figure 6. Evaluated IB system connections

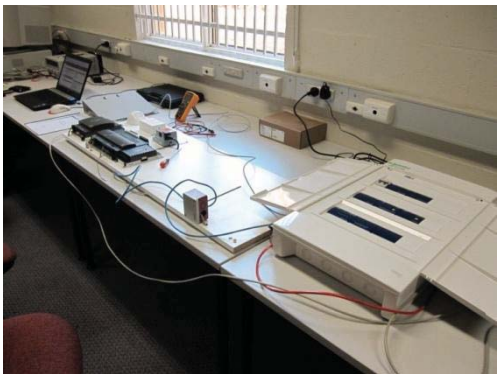

Figure 7. Evaluated IB system

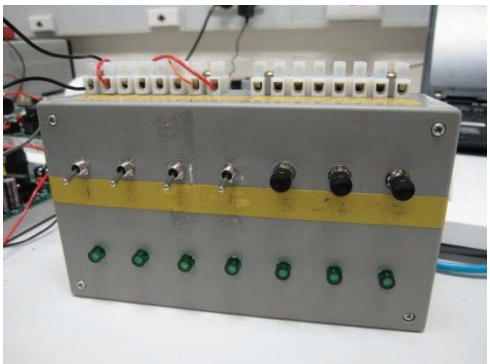

Figure 8. Evaluation input/output expansion module

The Management level Laptop was programmed to recognize all network items. A simple Graphical User Interface (GUI) was programmed for the Management software to monitor and control the various components (Figure 9). The GUI displayed items such as temperature readings from duct sensors, screen control of the VAV duct actuator, switch status, etc.

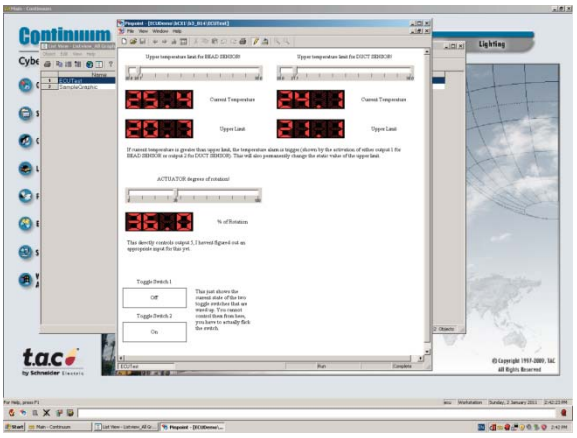

Figure 9. Management software graphical user interface

The emulated IB was then tested to the evaluation methodology (Figure 5), leading to the validation of a number of IB vulnerabilities (noted in Table 2).

RESULTS

The evaluation method was applied to the emulated IB, with some significant vulnerabilities found. These vulnerabilities included attacks on the physical management and automation level networks, attacks on the Controllers, and system reliance on power.

Physical access to the Workstation with common management level software was a significant threat against the IB. Such access allows the attacker to alter the IB program with their own coding, for example write to a Controller to allow an extended time delay before a detector alarms to support undetected access. In addition, there is the ability to install malicious code on the system, for example a key logger.

Physical access to any part of the Ethernet cable allowed wiretapping, for example using insulation-displacement connectors (Figure 10). Once connected to the Automation level network, freeware BACnet4Linux enables full monitoring capability; however, this software it its current format could not write back to control the IB system. Nevertheless, professional automation level software could not only monitor, but also write back to the IB system. At the Management ethernet level, the MS/TP protocol is readable using freeware such as Wireshark.

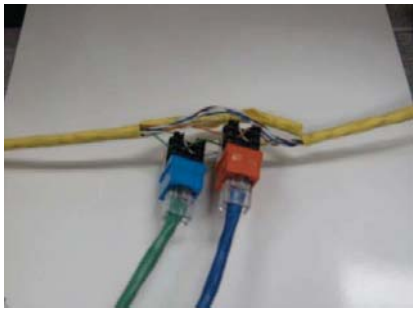

Figure 10. Wiretap covertly using single pair insulation-displacement connectors

Most IB Controller's contain a service port, where a readily available local Service Tool can be connected (Figure 11). The Service Tool allows local access to the Controller and changes to its automation level programming. For example, such program changes could switch inputs and outputs on or off at a predefined time, thereby turning off a detector or series of detectors to allow undetected access into a facility. Another example could be turning off HVAC and disabling any alarms, allowing server rooms to overheat and eventually, shutdown.

Figure 11. Service Port on a typical Air Handling Controller (AHC)

Controllers are supplied in a light-weight cover that is designed to provide protection for the internal circuitry, but not to protect against an attacker. The cover clips on/off by a simple depression of its sides and no form of anti-tamper is fitted. A significant redesign or use of an additional enclosure with anti-tamper would be required to protect the Controller.

Various Controllers had their literature reviewed for additional add-on wireless functionality. A wireless adaptor that plugs directly into the service port was found and such a device was covertly inserted within the Controllers enclosure.

The system relied on the primary power supply to maintain functionality, as all devices required some power to maintain monitoring and control capabilities. In general, power requirements varied between 240VAC to 12VAC/DC for devices. Loss of utility power can be localised or whole of system and when lost, other building plant and equipment fail such as HVAC, non-emergency lighting, elevators, etc. Loss or partial loss of IB power resulted in the loss of network communication, and control and monitoring capability.

Mitigating IB Vulnerabilities

Intelligent Building (IB) risks are contextual; in other words, directly aligned with the facility's threat exposure. If the facility contains sensitive or other highly protected information, the IB threat should be considered significant. However, there are a number of generic mitigation strategies that can be taken, such as:

- **Security risk management:** A sound security risk management strategy considering situational threat assessment, system criticalities and identified vulnerabilities.
- **Information system and communication protection:** Provide some degree of network isolation and partitioning, both internal and external, between the IB, operating systems and wider networks.
- **Physical and environmental security**: Control and validate access to the various and critical IB parts, with layered protection measures wherever possible.
- **Personnel security**: Ensure personnel are vetted who operate and maintain the IB system, including third parties.
- **Continuity of operations**: Provide a degree of emergency power to the more critical IB functions and parts.
- **Security awareness**: Provide training to increase awareness of IB and their vulnerabilities across the organisation. In addition, ensure greater integration of the various stove-piped departments such as IT and Computing, Physical Security, Personnel Security and Facility Management functions.

Future IB Threats and Risk

There needs to be some consideration of the future of Intelligent Building (IB) systems, to provide some degree of comment on developing and changing technologies likely to be used in the next decade. Such a review provides a degree of understanding of potential and developing threats and vulnerabilities of IB technologies. These issues (Table 3) should consider the greater use of wireless devices and telecommunications for ease of connectivity, greater and increasing open architecture, extended system communications, plug and play to facilitate connectivity, single design approach of such devices as Controllers, artificial intelligence and finally, smart and multi-functional sensors to achieve multiple functions.

Table 3. Future IB threats and risk

Future threat or risk	Descriptor
Wireless	Increasing use of wireless for ease and cost of connectivity
Open architecture	To aid increasing connectivity, both software and hardware architecture will need to become more available, allowing vulnerabilities to be found
Extended interconnectivity	Large systems will have multiple connectivity, both internal and externally, extending to other networks and cloud computing
Plug and play	Devices will be easier to install through plug and play, where devices are connected to the network and accepted with restricted authentication
Single design approach	A single Controller circuit that has multiple application use and functions. Functions may be software disenabled, such as wireless, various inputs & outputs, etc.
Artificial intelligence	Systems will become "smarter", leading to more complex systems and greater difficulty in identify vulnerabilities
Smart sensor	Sensors will perform multiple functions such as light, HVAC and security detection, making them more prone to spoofing or masking

FURTHER RESEARCH

There are a number of issues that need to be considered to mitigate current and future IB vulnerabilities, beyond only the technical and application issues of IB. Further research should consider:

- Dynamic technology of IB systems, considering the convergence between hardware, software and networks, and changing technology.
- Changing approaches to IB systems application, to better understand of how users, operators and integrators configure, install, operate and maintain IB.
- The IB industry's perspective and awareness of current and future security issues.
- Increasing the awareness of IB vulnerabilities to the various communities, such as security, IT and computing, infrastructure and facilities, etc.

CONCLUSION

Intelligent Buildings (IB's) are becoming more common place in commercial buildings. There are distinct benefits in IB's, such as reduced operating costs and a more reactive building, providing owners, operators and users a better experience. Nevertheless, IB's are prone to vulnerabilities across their hardware, software and network devices. The degree of vulnerability is contextual, primarily directed by the facility's threats. This study used a defeat evaluation method (Figure 4) to evaluate a list of proposed vulnerabilities (Table 2) using an emulated IB system to validate vulnerabilities.

The more significant validated vulnerabilities included attacks on the physical management and automation level networks, attacks against Controllers, and the IB's reliance on power to maintain capability. Wiretapping on the network allowed an understanding on what was occurring in the system. Access to Controllers also allowed access to the network, local programming, and its inputs and outputs. Nevertheless, mitigation strategies were proposed, including a threat informed security risk management process, understanding IB criticalities, some network isolation, staff vetting and access control, and raising awareness of IB vulnerabilities. Finally, future threats and risks considered the likely increase in wireless devices increasing open architecture and extended system communications, single design approach and smarter multi-functional sensors to achieve multiple functions.

REFERENCES

Automated Buildings.com. (n.d.). Networks. Retrieved July 22, 2010, from http://www.automatedbuildings.com/frame_products.htm

Brooks, D. J. (2010). *Assessing vulnerabilities of biometric readers using an applied defeat evaluation methodology.* Paper presented at the Proceedings of the 3rd Australian Security and Intelligence Conference, Perth.

CIBSE. (2000). *Building control systems: CIBSE Guide H*. Oxford: Butterworth-Heinemann.

Gadzheva, M. (2008). Legal issues in wireless building automation: an EU perspective. *International Journal of Law and Information Technology*, 1-17. doi: 10.1093/iijit/ean001

Jones, D. E. L., & Smith, C. L. (2005). *The development of a model for testing and evaluation of security equipment within Australian Standard / New Zealand Standard AS/NZS 4360:2004 - Risk Management*. Paper presented at the Recent advances in counter-terrorism technology and infrastructure protection, Proceedings of the 2005 Science, Engineering and Technology Summit 2005 Canberra, Australia.

Lafontaine, J. (1999). *Intelligent building concept*. Ontario: EMCS Engineering Inc.

Langston, C., & Lauge-Kristensen, R. (2002). *Strategic management of built facilities.* Boston: Butterworth-Heinemann.

Lonix Building Connectivity. (n.d.). System overview. Retrieved May, 25, 2010, from www.lonix.com/training/Lecture_Systems_Overview.pdf

Schneider, D., & Rode, P. (2010). Energy renaissance. *High Performance Building Magazine,* 13-16.

Schneider Electric TAC. (2004). *Product catalogue*: Schneider Electric.

Sharples, S., Callaghan, V., & Clarke, G. (1999). A multi-agent architecture for intelligent building sensing and control. *Sensor Review, 19*(2), 135-140.

Siemens. (n.d.). Communication. Retrieved July 22, 2010, from http://www.buildingtechnologies.siemens.com/bt/global/en/buildingautomation-hvac/building-automation/building-automation-and-control-system-europe-desigo/system/communication/Pages/communication.aspx

Smith, C. (2007). *The evaluation of security systems: Testing biometrics and intelligent imaging systems.* Paper presented at the The 6th International Workshop for Applied PKC (IWAAP2007).