2014

An analysis of security issues in building automation systems

Matthew Peacock
Edith Cowan University, m.peacock@ecu.edu.au

Michael N. Johnstone
Edith Cowan University, m.johnstone@ecu.edu.au

DOI: 10.4225/75/57b691dfd9386

AN ANALYSIS OF SECURITY ISSUES IN BUILDING AUTOMATION SYSTEMS

Matthew Peacock and Michael N. Johnstone
School of Computer and Security Science & Security Research Institute
Edith Cowan University, Perth, Australia
m.peacock@ecu.edu.au, m.johnstone@ecu.edu.au

Abstract

The purpose of Building Automation Systems (BAS) is to centralise the management of a wide range of building services, through the use of integrated protocol and communication media. Through the use of IP-based communication and encapsulated protocols, BAS are increasingly being connected to corporate networks and also being remotely accessed for management purposes, both for convenience and emergency purposes. These protocols, however, were not designed with security as a primary requirement, thus the majority of systems operate with sub-standard or non-existent security implementations, relying on security through obscurity. Research has been undertaken into addressing the shortfalls of security implementations in BAS, however defining the threats against BAS, and detection of these threats is an area that is particularly lacking. This paper presents an overview of the current security measures in BAS, outlining key issues, and methods that can be improved to protect cyber physical systems against the increasing threat of cyber terrorism and hacktivism. Future research aims to further evaluate and improve the detection systems used in BAS through first defining the threats and then applying and evaluating machine learning algorithms for traffic classification and IDS profiling capable of operating on resource constrained BAS.

Keywords
Building Automation, Intrusion Detection, Cybersecurity

BUILDING AUTOMATION SYSTEMS

The economic factors of production are land, labour, capital and enterprise. In business, the highest cost is the total employment cost of staff i.e. labour. The next highest cost is land, represented by buildings, either purchased or as rental costs. It is not surprising then, that many firms seek efficiencies in the use of the space they occupy by the use of Building Automation Systems (BAS). This drive for efficiency in heating, ventilation and air conditioning or HVAC is supported by the US Department of Energy (2010) who estimate that 29% of all electricity generated in the USA is consumed in buildings. Thus, BAS that measure and control buildings are becoming essential tools to manage energy usage and reduce operating costs.

The purpose of a building is to provide safety, security and comfort for workers, systems and goods which occupy the building. BAS are designed to fulfil these goals, through the use of automation to control and monitor building services. Originally, building automation applied only to HVAC systems, but the success in this system led to adoption across other building services. These systems include key services, such as lighting, water/waste management and more recently, safety and security services such as fire suppression systems, Closed Circuit Television (CCTV) and access control. Unfortunately, the lack of a holistic or strategic approach meant that each automated service was developed individually, using separate protocols, devices and physical media. Additionally, this lead to a number of terms used to refer to each automation system, such as Energy Management System (EMS), responsible for energy management, and Building Management System (BMS) which provided operational data logging for management (Fisk, 2012). When integration of building services into a centralised management system was proposed, the environment consisted of a wide range of protocols and devices, none of which were capable of being integrated together. This resulted in development of a range of new protocols that focused on integration and inter-communication; of which three major protocols emerged, namely, BACnet, KNX and LONworks. The remnant term BMS along with BAS and Intelligent Building (IB) are used interchangeably to refer to an integrated building automation system (Fisk, 2012), which is the focus of this research. The key success measure for these three protocols is their ability to communicate on multiple physical media, as shown in Table 1. Of these communication media, the ability to communicate over IP and similar protocols has resulted in BAS to often be connected to the corporate network, along with providing Internet facing connections for remote management. As these systems manage security and safety services, their principal requirements align with those of other control system network types such as Supervisory Control and Data Acquisition (SCADA). These cyber systems have physical ramifications in the event of failure, which can

impact not just the workers, systems and goods in the building, but also potentially external entities. The difficulty lies in implementing failure intolerance principles with failure tolerant Information Technology (IT)-based systems. The remainder of this paper details the security issues present in BAS.

Table 1: Comparison of BAS Protocols with supported Physical Media and Networking Protocols

	Physical Media					**Networking Protocols**			
BAS Protocols	Optical Fibre	Twisted Pair	Power line	Radio Frequency	EIA-485	802.15.4	ARCNET	UDP/IP	Ethernet
BACnet	X	X	X	X	X	X	X	X	X
KNX	X	X	X	X				X	
LONworks	X	X	X	X				X	

SECURITY ISSUES

Much like the advancement of other service-based systems, BAS were not designed with security as a paramount requirement. Early security of these systems revolved around isolationism through physical security and obscure proprietary protocols. While these measures were acceptable when automation systems were not interconnected, security has not been applied to the new integrated BAS depicted in Figure 1. The key features of the integrated BAS, are a predominately centralised system, external facing connections and internal connections to the enterprise network. This has created a large attack surface for BAS, and therefore presenting a ripe target for terrorist/hacktivists-motivated cyber attacks. Further, while BAS have similarities to IT networks, the same security mechanisms cannot be directly applied as there are domain-specific concerns as noted by Granzer and Kastner (2010). Due to the encapsulation of BAS protocols inside IP, prevention and detection systems must be adjusted to interpret and recognise these protocols. Additionally, the strict bandwidth and processing requirements of these systems often prevents the use of confidentiality processes, such as encryption, although Antonini et al. (2013) suggest that, with protocol redesign, effective cryptography can be implemented on low-power processors. Moreover, the high availability requirement of BAS does not align with the patching philosophy in IT systems, with BAS either not being patched, or being exposed for long periods of time while patching is scheduled (Cheminod et al., 2013). The exposure caused by lack of updates is further exacerbated by BAS manufacturers failing to certify patched systems in a timely manner, if at all. This leads to the risk of warranty defaults which no building manager wishes to cause due to liability issues. Thus there is a certain tension between the IT security function and the building supervisory management function.

Granzer and Kastner (2010) examined the BAS protocols in table 1 (and additionally, ZigBee) with respect to their fulfillment of security requirements such as authentication, authorisation, confidentiality and integrity. Interestingly, they found that of those protocols, ZigBee met the most security requirements, with BACnet a close second. It is perhaps not surprising that Park et al. (2007) tested running BACnet over ZigBee, using the ZigBee protocol as one of the data link layer protocols in a BACnet system.

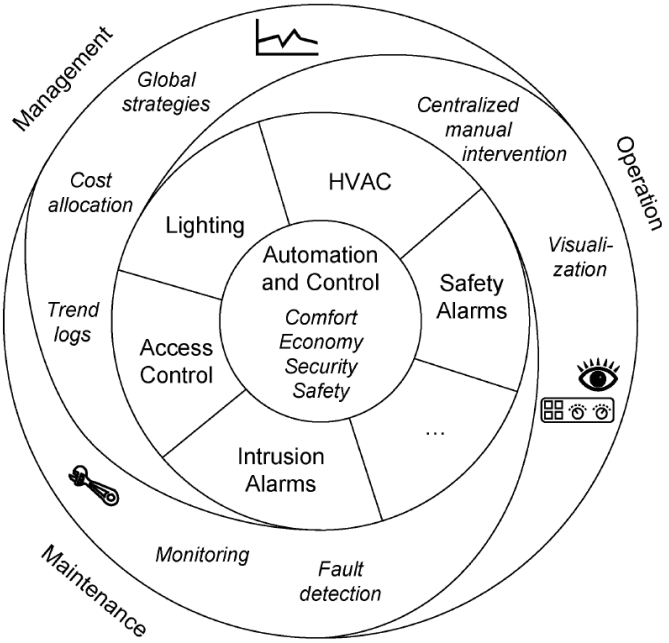

Figure 1: Integrated Building Automation System, adapted from Kastner (2005)

Protocol Design

Secure design has not evolved into BAS, with large levels of trust still placed in users and devices to account for legacy and poorly integrated systems. Similar to SCADA, the life-cycle of systems and devices in BAS is much longer than IT systems. BAS devices are expected to last upwards of a decade, while maintaining high availability, resulting in legacy systems that are often un-patched, leading to increasing exposure to vulnerabilities over time. The encapsulation of BAS protocols in IP and related protocols has resulted in the inheritance of the known security weaknesses in said protocols. Further, similar security pitfalls have befallen BACnet, KNX and LONworks protocol design. KNX security revolves around simple access control mechanisms that transmit passwords in plain text over the networks, with guidelines promoting isolationism through the use of firewalls and security through obscurity. LONworks security practices are slightly more robust, with Message Digest algorithm 5 (MD5) hashing paired with a shared secret used for authentication. Key distribution however is left up to the implementer, along with the lack of confidentiality provided by using MD5, with its possibility of hash collisions. In comparison, BACnet has a much wider security implementation, which has evolved, albeit it slowly, in-line with BAS. Provided as BACnet Security Addendum g, BACnet Security Services (BSS) are implemented in the network layer of the BACnet stack. BSS provides encryption through Advanced Encryption Standard (AES), and Key Hashed Message Authentication Codes through MD5 and Secure Hash Algorithm 256bit (SHA256). The caveat however, is that BSS are an optional feature of the protocol, to account for legacy systems not capable of processing encryption (Cheminod et al., 2013). As noted by Michael Newman, the leader of the BACnet working group from 1987 to 2000, "...no company has yet implemented it [BSS] in a commercially available product. This could change, of course, but so far I don't believe you can buy a product that implements the BSA" (Newman, 2013, pp 44). Of the three protocols, BACnet is the dominant protocol used in the US, China and Australia, with KNX primarily used in Europe, where that standard was defined. A decade ago, LONworks was used in the majority of US BAS, however the success of BACnet has lessened the dominance of LONworks (Kastner et al., 2005, Novak & Gerstinger, 2010, Cheminod et al., 2013).

In response to the protocol security problems outlined above, Antonini et al. (2013) proposed a secure communication protocol for BAS which provides security guarantees against an attacker able to eavesdrop on all transmissions. They provided a case study as proof-of-concept of the protocol using KNX as the target.

Awareness and Detection

The lack of security implementations in BAS can be traced to the aforementioned trade-off between security and function. Noted by Cheminod et al., (2013) operators of these systems believe that processor data is of no value to an attacker, and thus security need not be implemented. While temperature sensor readings for the air-

conditioning unit in an office may seem innocuous, what of the security and safety services, where financial and reputation impact can occur? Preventing a fire suppression system from activating during a fire, or opening secure area doors at night for theft are potential issues. Additionally, consider a Stuxnet type attack, where the field reading data were manipulated to show expected readings while the controller actually sabotaged the nuclear enrichment process. A similar attack could be crafted against building sensors without knowledge of the BAS operators.

The next notable lack in BAS security is detection of potential attacks. The benefits of Intrusion Detection Systems (IDS) in enterprise networks have been well-documented. Further, as stated by Skopic (2014), all modern control systems are applying IDS in response to the rising threat against critical infrastructure. The same statement cannot be made for BAS, with immature progress in research towards detection implementations for BAS protocols. Discussion of IDS in BAS by Granzer (2010) notes the benefits of anomaly detection IDS, due to its reduced overhead on the network compared to a signature based approach, which must store signatures and therefore recognises only the "known unknowns". Both network flows (Krejvci et al., 2012) and packet inspection (Wendzel et al., 2012) methods have been implemented using BACnet and KNX respectively, with recognisable patterns identified using network flows, particularly on a week-to-week comparison. The activity profile of BAS is dependent on the service in use, with lighting, water management and access control systems having peaks during business hours, and troughs out of business hours; in comparison monitoring systems such as CCTV have a different network pattern. These findings align with the physical interaction between those occupying the building and these services, where actions directly influence the activity in each building service. Coupled with the wide combination of devices and physical media that comprise BAS, each implementation of BAS is unique. With uniqueness comes the requirement for fine-tuning detection implementations to match the system, additionally, due to human interactions within the system, the definition of normal behaviour (pattern) can shift. Tuning an IDS is often a manual process, however, machine learning algorithms can potentially be applied to traffic classification and profiling, similar to implementations in enterprise IDS and those implemented on wireless sensor network.

In relation to detection, awareness of the existing threats forms a significant part of the risk assessment of a system. The threats against BAS have not been evaluated using a weighted or state-based model. For threats to be quantified, a weighting must be applied to determine the criticality and probability of an event occurring. The complexity of system implementation in BAS can cause risk assessments to have increased cost and length compared to enterprise network assessments. Additionally, due to BAS containing security and safety critical systems, defining the cost of environmental damage or loss of life is often not appropriate (Cheminod et al., 2013). A further complication, caused by the aforementioned focus on function rather than security, is that security professionals are unused to the domain of BAS therefore effective assessments are difficult to procure.

Attack trees are a tool that are often used in the security domain to visualise a structured approach to protocol, system and network weaknesses (Byres et al., 2004; Khand. et al., 2009). The results of attack trees can provide detailed insight into potential risks and vulnerabilities detected. Applying a weighting determining the success rate of attacks based on variables, such as technical expertise, probability of detection, cost of attack and system complexity, results in a numeric value, from which the most efficient path to a successful attack can be determined and mitigated.

The lack of security in control systems provides the potential for a number of IP-based security attacks to occur. These include, but are not limited to, denial of service, man in the middle, data tampering and data ex-filtration, which impact the confidentiality, integrity and availability of buildings operating BAS. These threats have been noted by the US Government, with the National Institute for Standards and Technology (NIST) releasing a draft in February 2014 of the Framework for Improving Critical Infrastructure Cybersecurity (NIST, 2014). The aim of the framework is to provide a set of industry standards and best practices to help manage cybersecurity risk, which can be applied to BAS. This is at least a start to addressing the potential types of risks associated with BAS, defining the known knowns, and implementing safeguards and mitigations to address these identified risks.

CONCLUSION

The current state of BAS security or lack thereof has resulted in the potential for extensive security breaches to occur. Security implementations inside the protocols managing building services are significantly lacking, or not widely used, relying on IT-based security solutions. The problem exists that IT-security implementations cannot be directly applied to BAS due to specific domain concerns, such as differing requirements and plethora of devices and protocols present in these networks. Additionally, the uniqueness of each BAS, with its combination of physical media, protocols and devices effectively precludes a universal approach to security (the domain-

specific and familiarity arguments presented above). With the increasing threat of terrorism and hacktivism, physical repercussions from cyber attack is an increasing concern. While security in SCADA systems managing critical infrastructure is improving, awareness has not arrived for those in the building automation sphere, where 2014 technology is being used with 1990s security practices. Security principles should be applied to BAS in a proactive way, before a major cyber incident and without the need for a catalyst such as 9/11 in the aviation industry.

Future Work

Using a weighted attack tree model, future work will consist of defining a comprehensive review of the known threats against building automation systems, particularly those using the BACnet IP protocol. Further to this, said known attacks will be modelled in a test bed BACnet controlled BAS network to generate malicious network traffic. In addition to this malicious traffic, normal operating traffic will also be recorded for the application of machine learning algorithms for traffic classification. This modelled traffic will be used to analyse and compare a number of machine learning algorithms to determine the most effective and efficient for detection techniques.

REFERENCES

Antonini, A., Barenghi, A., and Pelosi, G. (2013). Security Analysis of Building Automation Networks – *Threat Model and Viable Mitigation Techniques. ;In Proc. NordSec 2013. Pp.199-214.*

Byres, E. J., Franz, M., & Miller, D. (2004). The use of attack trees in assessing vulnerabilities in scada systems. *In Proceedings of the International Infrastructure Survivability Workshop*.

Cheminod, M., Durante, L., & Valenzano, A. (2013). Review of security issues in industrial networks. *Industrial Informatics, IEEE Transactions on, 9 (1), 277-293. doi: 10.1109/tii.2012.2198666*

Fisk, D. (2012). Cyber security, building automation, and the intelligent building. *Intelligent Buildings International, 4 (3), 169-181. Retrieved from http://dx.doi.org/10.1080/17508975.2012 .695277 doi: 10.1080/17508975.2012.695277*

Granzer, W. and Kastner, W. (2010). Security Analysis of Open Building Automation Systems. *In Proc. 29th International Conference on Computer Safety, Reliability and Security (SAFECOMP '10), pages 303-316,*

Granzer, W., Praus, F., & Kastner, W. (2010). Security in building automation systems. *Industrial Electronics, IEEE Transactions on, 57 (11), 3622-3630. doi: 10.1109/tie.2009.2036033*

Kastner, W., Neugschwandtner, G., Soucek, S., & Newmann, H. (2005, June). Communication systems for building automation and control. *Proceedings of the IEEE, 93 (6), 1178-1203. doi: 10.1109/JPROC.2005.849726*

Khand, P. (2009, Feb). System level security modeling using attack trees. *In Computer, Control and Communication, 2009. ic4 2009. 2nd International Conference on (p. 1-6). doi: 10.1109/IC4.2009.4909245*

Krejci, R., Celeda, P., & Dobrovolny, J. (2012). Traffic measurement and analysis of building automation and control networks. *In Dependable Networks and Services (pp. 62-73). Springer.*

Newman, H. M. (2013). Bacnet: *The global standard for building automation and control networks.*

NIST. (2014) Framework for Improving Critical Infrastructure Cybersecurity. Retrieved from: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf

Novak, T., & Gerstinger, A. (2010). Safety- and security-critical services in building automation and control systems. *Industrial Electronics, IEEE Transactions on, 57 (11), 3614-3621. doi: 10.1109/tie.2009.2028364*

Park, T.J., Chon, Y.J,, Park, D.K. and Hong, S.H. (2007). BACnet over ZigBee, A new approach to wireless datalink channel for BACnet. *Proc. 5th IEEE International Conference on Industrial Informatics, pp.33-38.*

Skopik, F., Friedberg, I., & Fiedler, R. (2014, Feb). Dealing with advanced persistent threats in smart grid ict networks. *In Innovative Smart Grid Technologies Conference (ISGT), 2014 ieee pes (p. 1-5). doi:10.1109/ISGT.2014.6816388*

US Department of Energy (2010). *Buildings Sector Energy Consumption*. Buildings Energy Data Book. Available from: http://buildingsdatabook.eren.doe.gov/TableView.aspx?table=1.1.1

Wendzel, S. (2012). Covert and side channels in buildings and the prototype of a building-aware active warden. *In Communications (icc), 2012 IEEE International Conference on (pp. 6753-6758).*