Securing a Building Automation and Control System from Cyber Attacks

Nils T Siebel

Department of Engineering, HTW University of Applied Sciences Berlin, Berlin, Germany

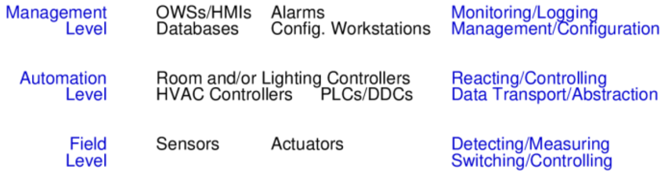
Abstract—Cyber attacks on IT systems are common and usually originate from the Internet. Building automation and control systems (BACs) are often connected to the Internet but lack strong protection against these attacks: weak and/or default passwords, non-encrypted communication and lack of protection against unauthorised changes to data and programming are widespread. In this article we discuss how BAC systems can be protected against cyber attacks. This includes an assessment of IT security features of standards like ASHRAE 135 (BACnet) and ISA/IEC-62443.

Keywords—*Cyber security; building automation; automation and control systems; hackers; BACnet*

I. Introduction

Modern buildings contain technology to automatically regulate temperature, control shading and lighting. This automation technology runs heating systems in winter and regulates A/C systems in summer. Collecting meter data allows the optimisation of energy consumption; extra sensors like motion detectors can both switch off light when not needed and help keep the building secure from intruders. Safety is ensured by using even more sensors like smoke and gas detectors as well as alarms.

Sensors collect data, actuators allow acting on them by switching, regulating and by driving moving parts like valves. These sensors and actuators are controlled using building automation controllers; together they form a "building automation and control system" (BAC).



Management Level	OWSs/HMIs Databases	Alarms Config. Workstations	Monitoring/Logging Management/Configuration
Automation Level	Room and/or Lighting Controllers HVAC Controllers	PLCs/DDCs	Reacting/Controlling Data Transport/Abstraction
Field Level	Sensors	Actuators	Detecting/Measuring Switching/Controlling

Figure 1: Three-Level Building Automation Model

The devices that make up a BAC are usually grouped into three levels, as shown in Fig. 1. Realisation at the lowest, field level is achieved either through direct communication between the sensors and actuators (e.g. switch controls light) or by going through a CPU element like a programmable logic controller (PLC) or direct digital control (DDC). The three levels may contain devices as follows :-

1. Field level – sensors and actuators without "intelligence" that do now have an overview of the system.
2. Automation level – Controllers (PLCs or DDCs) allow control of heating, ventilation and air conditioning (HVAC) systems; control for functions like corridor lighting and shading for façades. Also, realisation of simple control functionality like room controllers that regulate lighting as well as HVAC aspects of a single room. They may collect data (e.g. meter or usage data) from field level devices and make them available to the …
3. Management level – Where the data is collected, stored in databases and displayed to users using human machine interfaces (HMIs) or operator workstations (OWSs), sometimes including alarms. Here you will also find configuration and programming interfaces for the system.

Data connections between field devices and from field devices to automation devices are implemented using either data buses or direct analogue/digital signalling. Analogue measuring/control signals often have ranges like 0-10V, 1-10V, 0-20mA and 4-20mA while digital ones use 0/5V, 0/24V or NAMUR signalling (which allows the detection of faults). Data buses used in BACs include DALI (for lighting), KNX (mainly for lighting and shading), M-Bus (for metering), MP-Bus (for valves) and LonTalk (mainly for HVAC) as two-wire signals, as well as wireless signals like EnOcean and ZigBee.

The two upper levels communicate using IP-based standards, BACnet/IP [1] being the most modern and feature-rich, but also using Modbus/IP and Ethernet/IP. Web interfaces to automation and management level devices are also becoming more and more commonplace.

In this article we will analyse attacks on BAC systems and discuss countermeasures. This includes discussion of common attacks in the Internet and an analysis of BAC devices and communication channels for attack surfaces. A discussion of suggested standards on BAC cyber security like the BACnet addendum g and ISA/IEC-62443 is also included.

II. Common Cyber Attacks

A. *Developments in the Hacker Scene*

In the past the hacker scene was different in nature. You would hear about young, intelligent people hacking for fun, to show that they can, to expose companies not securing their systems – and often not for financial gain. Government hacking was not discussed in the press.

Nowadays hacking activity by governments or associated institutions is widely known and talked about; even their hacking tools have been exposed. Any small-time criminal can buy and download hacking tools on the Internet (e.g. in forums on the "dark web", i.e. hidden areas in the Internet) and become a "hacker" (others would say "only a script kiddie") without understanding much about the tools they use.

B. *Attack Types*

Common attacks on computer systems focus on servers and desktop systems as well as on network infrastructure or IoT (Internet of things) devices.

Servers are attacked for their web presence; being exposed to the Internet by design means they have a great "attack surface". Hackers try to take over whole servers or single accounts in order to profit by using their e-mail capabilities and/or web space, usually for sending spam. Attacks commonly work by trying out passwords ("brute force" guessing) for mail/web logins, or use commonly known weaknesses in CMS-based web sites like those using Wordpress, Joomla, Drupal etc. [2]. Another important attack on servers is targeting databases and other monetisable information, the biggest known being the Yahoo break-in in August 2013 were all 3 billion user accounts were compromised, their data for sale in the dark web [3].

Desktop systems are usually attacked in order to extract money from their users. This can be achieved by stealing personal data like credit card and bank data, social security numbers and passwords. Another popular method is to install a virus that encrypts or deletes important user files and than shows a ransom message. It says that in order to get back the files (which may or may not actually be possible) the user is supposed to pay money to the attacker via the Internet. Malicious software – a.k.a. "malware" – like this is called "ransomware" and is in most cases distributed via e-mail (in an attachment using a security hole in MS Office or Acrobat Reader) or hidden in web pages (using vulnerabilities in the web browser or its plugins; attacks are easiest when Adobe Flash Player or Oracle Java plugins are installed or MS Internet Explorer is used [4,5]). Once inside a local network (LAN) malware can often spread easily, e.g. using security holes or open access policies in MS Windows operating systems.

In the past months hospitals [6] and other companies were also attacked by ransomware, resulting in one instance in up to $300m estimated loss by a big shipping company [7]. It should be noted that most companies do not publish attacks or the resulting loss.

Most attacks on IoT and network infrastructure devices focus on cable/DSL routers and IP cameras. These devices are connected to the Internet around the clock. They often lack proper security configuration, having no, or a well-known default password set, or they have other security holes. Vendors traditionally do not fix security issues in all of their devices currently in use, especially to older hardware if newer models are out. Even of they do publish updates to firmware, devices are not updated because they either do not check for and install new firmware automatically or users are not aware of the necessity (and way) to install updates. Once hacked, devices can be used to attack other devices (worm-type behaviour) and they can together form a botnet.

IoT botnets are networks of these hacked IoT devices responding to commands a single attacker. They routinely query "command and control" ("c&c") servers for new information what to do. The main activity are DDoS attacks, that is, distributed (first "D") attacks on a single target, trying to cripple it by flooding it with requests, resulting in a denial of service ("DoS"). As an example, a website could be attacked [8], or a game server [9], or a DNS service [10], resulting in the inaccessibility of parts of the Internet.

III. Attacks on Building Automation Systems

A. *Risks*

Especially the prevalence of and profit to be gained from operating IoT botnets makes BACs more and more interesting from the point of view of an attacker. Industrial espionage and sabotage of BAC or other automation devices can also result in crippling losses for a company.

Securing BACs from cyber attacks is therefore important, but very difficult for several reasons:

- They operate close to the public (e.g. in companies, hospitals and prisons)
- They are designed for autonomous operation, which also means that operators do not often check devices for the presence of attacks, or install security updates
- Security updates may result in the necessity to have a new final acceptance or certification of the overall system, which is sometimes a reason not to install them even if they do exist
- Product life cycles in building automation are 10 or more years which is very long considering IT components and software used
- There is no tradition of secure designs in BAC hard- or software; they are protected by a password at best – but this is sent over a non-encrypted line.

B. *Goals*

When securing any data or system one must analyse the types of attacks to be expected, the attack surface (possible entry into the system) and state the goal of the safeguarding action.

The following basic security aspects are usually considered during analysis [11, chapter 2]:

1. Confidentiality – restricting access to information and systems, e.g. by encryption of data and password protection
2. Integrity – ensuring that data is not changed (at least not without detection), e.g. when looking at an online banking website or the web interface of an intrusion detection system
3. Availability – systems and data are accessible when needed; DDoS and ransomware attacks (both mentioned above) are typical attacks on availability of data and systems, but a power outage may achieve the same thing.

Sometimes further aspects are considered, like authenticity, e.g. data origin authenticity which implies that the recipient of a message can check whether the data stems from the correct sender. However, adding more items to the list than the three above changes the catchy acronym "C-I-A".

Applying the C-I-A aspects to a BAC system one can derive protection goals as these:

1. Confidentiality – Only authorised parties can read data exchanged between devices or between a user and a device. This includes the protection of any remote maintenance or data connection which will contain authentication data like passwords. Data at rest can be encrypted in addition to communication channels if an attacker can gain physical access to data storage devices.

2. Integrity – Data like measurements, but also programming/configuration data as well as device firmware are not changed without authorisation.

3. Availability – Data and devices are ready to be accessed / to work at all times. One needs to protect against DDoS attacks, defects, deletion of data and programming, network disconnection and power loss. Servers required by devices (like database servers) and by people (like web servers) need to be available.

C. *Attack Surfaces of BAC Systems*

Possible points of attack are very much dependent on the system under consideration. For example, a BAC system in a prison may be in danger of being manipulated by inmates in order to open doors or stir unrest. This could include tampering with fire alarms (at the field bus level) or severing connections. Similarly, in a treatment centre for (criminal) alcoholics, presence and alcohol detectors have been tampered with in the past to bypass regulations. Even one or more non-handled faults could trigger an undesired situation, e.g. when no backup staff is available to ensure a smooth operation.

Attacks by people having physical access are very difficult to defend against. This can include workers or ex-workers wanting to cause damage, for example as a type of “revenge” after being laid off or denied some wish. They may, of course, also be paid to do destructive or espionage work, like collecting data for a competitor.

In any system using wireless networks to integrate sensors or actuators the connections can be severed with ease from several meters away – which is why security related devices should always to be connected by cable. Even if most thieves have not yet upgraded to wireless jamming equipment it may only be a question of time – wireless burglar alarms sell well due to their easy installation.

Considering an IP-based BAC installation in a hospital, it can prove very difficult to keep patients from accessing the network when there may be network printers in the corridors or network sockets in the patients’ rooms. Most patients, of course, will mainly seek Internet access to pass the time and save mobile fees. They may, however, inadvertently spread viruses from their Windows laptops or saturate the network (⇒ availability problem).

In general, one may distinguish further points of attack wherever access is possible:

- Physical access to devices or network (with little chance of defence)
- BAC components sharing a network (usually, IP) with PCs, especially office PCs with e-mail and web browsing functionality
- BAC systems exposed to the Internet, e.g. for remote maintenance or monitoring like energy management [12]
- Laptops and other devices of maintenance personnel sharing the network temporarily.

Attack surfaces need to be considered over the whole lifetime of all components of the system. This may begin the time building controllers (e.g. room controllers or DDCs) are installed in the suspended ceiling of an unfinished building (where it is very difficult to monitor who accesses it) up to an analysis of possible attacks on laptops used during maintenance of BAC components much later during their life cycle.

D. *Security by Obscurity*

Often access to information and systems is hidden instead of encrypted or otherwise technologically secured, e.g. by using a non-standard IP port number to connect to an administration interface, or a “secret” URL that allows only people who know about it to execute a system command. There even used to be a case where the login password was written in the source code of the login HTML page – usually invisible, but clearly visible for people who looked at the source. The login password was checked by JavaScript code on the web page itself.

As an example for a system not secured against outside access or tampering, Fig. 1 shows a publicly accessible web interface to the ventilation control of a public indoor swimming pool in Austria (rough translation in italics). No password was required to get to the screen shown here where everyone could control the ventilation. In other screens, more HVAC components including the pool temperature could be adjusted. This may seem unimportant and most people who find this by accident would never change any setting. However, a criminal could see personal gain in this, whether it be for ransom, sabotage or to cause public disturbance.

The apparent security gained from obscurity by simply hiding information does not work at all against attackers who own a computer. Computers can try out all possible IP port numbers, they can try out popular URLs and automatically generate even more. Looking at the source code of an HTML page is part of the standard analysis of an attacker.

A special online search engine for automation systems, including BAC systems, regularly lists tens of thousands of these systems, often connected to the Internet for remote maintenance. Many of these do not hide sensitive data about the building or automation plant they represent and some even allow full remote access without a password – like the one shown above.

IV. SECURING A BAC SYSTEM

In order to consistently make BAC systems more secure against cyber attacks one needs to establish a process governing production, possibly also the supply chain, installation, configuration/programming, operation and maintenance. International standards like ASHRAE 135 (BACnet) addendum g [13] and ISA/IEC 62443 [14] can help to both cover many security aspects and make conforming devices interoperable, albeit they sometimes do not tell you how to achieve these goals.

A. *BACnet Addendum g*

BACnet [1] is the best standard for interoperability and manageability of a BAC system – even across vendor boundaries. It defines data objects, their properties as well as services for communication. Unlike other standards (like Modbus) it has been written specifically for building automation systems, not automation and control systems in general. This means it has all necessary definitions and data types. It also makes documentation and analysis easy by its object centred, open design and management services.

In 2010 ASHRAE published the addendum “g” to the standard to ensure IT and data security aspects of BACnet devices and communication channels. This was difficult because of several reasons. For one, it has a very open design, exposing devices and data for reasons of easy management and interoperability. For another, its IP-based communication (BACnet/IP) is based on UDP/IP while most secure communication and authentication standards (like TLS and

SSH) are (in its standard form) based on TCP/IP and can therefore not easily be used by BACnet. ASHRAE 135g instead defines its own protection mechanisms which makes its implementation more cumbersome.

The standard defines, among other things:

- Data confidentiality and integrity
- Authentication for peer entities, data origin and administrative access [13].

Security is realised on the network layer and is defined for all media, like MS/TP, BACnet/IP etc. and all device types. It also works for all services/packets including confirmed and unconfirmed messages, unicast and broadcast.

1) Features and Assessment

ASHRAE 135g allows the use of MD5 and SHA-256 (i.e. SHA2 with 256 bits) hashes. MD5 is broken [15] but SHA-256 is considered safe for use. For confidentiality by encryption it allows symmetric encryption with the AES-128 standard which is also good by current security standards. 135g has (and requires) a somewhat complex key management, but thereby enables layered protection of access to the bus (communication), data (confidentiality) and device configuration.

AES is also used for signatures for proofs of authenticity of data and devices. A device can check whether a communication partner is authentic or an attacker disguising themselves – a man-in-the middle-attack [11]. Authentication would normally be realised with a public key (i.e. asymmetric) cryptography algorithm like RSA, as used in standards like HTTPS, PGP etc. In comparison with modern, secure asymmetric algorithms, AES has the advantage of being much less computationally demanding, its execution further accelerated by special AES instructions in modern embedded CPUs. This speed advantage may well have been the reason for choosing AES for signatures.

Authenticity checking, as well as access protection by keys, can also prevent unauthorised change of data, programming and firmware, which is an important feature.

Overall, ASHRAE 135g seems to cover all important aspects needed for cyber security in BAC systems (except perhaps the availability aspect which demands other techniques that do not fit in this context anyway). So far only one device exists which implements the standard – a gateway by the German company MBS – but since the demand for protection against cyber attacks is growing one can expect more devices in the near future.

B. IEC 62443

The IEC 62443 standard was created originally as ISA-99 by the International Society of Automation (ISA) but is now further developed by the International Electrotechnical Commission (IEC). Currently the standard is still work in progress; some of its parts still have draft status or are being developed.

The standard consists of 13 parts in 4 categories:

- General, which covers concepts, metrics, models and terminology
- Policies and Procedures, covering security management, installation and maintenance aspects
- System Requirements, which focuses on technologies, networking as well as access management; and
- Component Requirements, which will, among other things, address development aspects of secure automation systems.

IEC 62443 thus covers a wide area, including many recommendations for business processes and best practises, from infrastructure and access control to backups to ensure availability.

The standard was written for automation and control systems in general, not specifically building applications. Applying it to the building setting would, however, be possible. This is especially true for management aspects and subjects like access control and secure networking. It may not introduce new communication standards between devices, so a combination with ASHRAE 135g (which does not cover nearly as many management aspects) could be possible and useful.

As a relatively new and not yet final standard IEC 62443 is difficult to finally assess. It is quite extensive and will have to be reviewed and tested in the real world. Nevertheless it looks very promising.

C. Other Aspects of Cyber Defence

When securing a BAC system standard techniques and best practises from the IT world can and should be applied.

For example, if the system needs to be accessed from the Internet, whether it be for remote maintenance, data access or control, one can use VPN (Virtual Private Network). A VPN access can be implemented in a network router on-site. The BAC devices would be configured and connected such that no direct outside access is possible, however, they are connected to (or by) the router. VPN could then be used to access the router from the outside using an encrypted and secured channel. Once a device has gained this access the router virtually makes it part of the local network, thereby allowing communication with all BAC components.

Hardening techniques as used in standard servers and networks can also be used, for example

- Reducing physical and electronic/IT access to only the minimum required for proper operation
- Closing, disabling and removing network ports, software, services and everything else not needed, including telnet, ftp, Modbus and configuration/ programming services and ports on controllers
- Choosing good, individual access passwords and distinct user levels e.g. for viewing, configuration/ control and re-programming
- Disabling the possibility of guessing passwords quickly by using brute force, by rate-limiting login attempts and automatic, dynamic blocks
- Separating network parts that do not need to communicate, e.g. office networks, guest networks, staff WiFi and BAC networks by using VLANs, and perhaps in addition using DMZs (demilitarised zones) for restricting online access
- Using good and well-configured firewalls to filter both incoming and outgoing traffic
- Keeping other computers on the same site, as well as laptops used for maintenance, secure.

V. CONCLUSIONS

Cyber security for buildings is becoming more and more important as attacks increase. Technological defence solutions include standard network security technology as used in the IT industry but can also use special devices like those adhering to the BACnet addendum g standard. Managerial defence aspects are covered in IEC 62443 but also in other, national and international recommendations as those some governments issue for use in critical infrastructures. Efficient and effective defence against cyber attacks is difficult but possible for BAC systems. However, the technology used in most current BAC devices does not enable effective protection due to the use of old, non-secure standards and techniques.

Acknowledgements

The work of those journalists exposing details of hacking activities is gratefully acknowledged; without them most of the information in the first part this article would not have been available to write about.

Names of companies and products used in this article may be trademarks of their respective owners even if not marked as such.

References

[1] ISO 16484-5 / ANSI/ASHRAE Standard 135: A Data Communication Protocol for Building Automation and Control Networks, International Organization for Standardization, Geneva, Switzerland, 2003–/1995–.

[2] Sucuri Inc., "Website Hacked Trend Report 2016 – Q1", online report, USA, May 2016. https://sucuri.net/website-security/website-hacked-report/

[3] Selena Larson, "Every single Yahoo account was hacked - 3 billion in all", online article, CCN Money, USA, October 2017. http://money.cnn.com/2017/10/03/technology/business/yahoo-breach-3-billion-accounts/

[4] Brian Krebs, "Flash Player is Dead, Long Live Flash Player!", online article, Krebs on Security, USA, August 2017. https://krebsonsecurity.com/2017/08/flash-player-is-dead-long-live-flash-player/

[5] Brian Krebs, "Good Riddance to Oracle's Java Plugin", online article, Krebs on Security, USA, February 2016. https://krebsonsecurity.com/2016/02/good-riddance-to-oracles-java-plugin/.

[6] Marcus Hutchins, "NHS cyber attack: Everything you need to know about 'biggest ransomware' offensive in history", online article, The Telegraph, UK, May 2017. http://www.telegraph.co.uk/news/2017/05/13/nhs-cyber-attack-everything-need-know-biggest-ransomware-offensive/

[7] Iain Thomson, "NotPetya ransomware attack cost us $300m – shipping giant Maersk", online article, Forbes, USA, August 2017. https://www.forbes.com/sites/leemathews/2017/08/16/notpetya-ransomware-attack-cost-shipping-giant-maersk-over-200-million/

[8] Dan Goodin, "How Google fought back against a crippling IoT-powered botnet and won", online article, Ars Technica, USA, February 2017. https://arstechnica.com/information-technology/2017/02/how-google-fought-back-against-a-crippling-iot-powered-botnet-and-won/

[9] Brian Krebs, "Who is Anna-Senpai, the Mirai Worm Author?", online article, Krebs on Security, USA, January 2017. https://krebsonsecurity.com/2017/01/who-is-anna-senpai-the-mirai-worm-author/

[10] Larry Dignan, "Dyn confirms Mirai botnet involved in distributed denial of service attack", online article, ZDNet, USA, October 2016. http://www.zdnet.com/article/dyn-confirms-mirai-botnet-involved-in-distributed-denial-of-service-attack/

[11] William Arthur Conklin, Gregory B White, Dwayne Williams, Roger Davis and Chuck Cothren, "Principles of Computer Security: CompTIA Security+ and Beyond", 2nd ed., McGraw-Hill Publishing Company, New York, USA, 2009.

[12] ISO 50001:2011 Energy management systems – Requirements with guidance, International Organization for Standardization, Geneva, Switzerland, June 2011.

[13] Addendum g to ANSI/ASHRAE Standard 135.1-2009, American Society of Heating, Refrigerating and Air-Conditioning Engineers, New York City, USA, June 2010.

[14] IEC 62443 Industrial communication networks – Network and system security, set of norms, International Electrotechnical Commission, Geneva, Switzerland, 2009- (some parts still have a draft status).

[15] Ronald L Rivest, "hashlib – faster md5/sha, adds sha256/512 support", mailing list message, Python-Dev mailing list, December 2015, https://mail.python.org/pipermail/python-dev/2005-December/058850.html