(in)security in building automation
how to create dark buildings with light speed

Thomas Brandstetter,[1][2] Kerstin Reisinger[1]

Abstract:

The usage of building automation, regardless if in private homes or corporate buildings, aims to optimize comfort, energy efficiency and physical access for its users. Is cyber security part of the equation? Unfortunately, not to the extent one might expect, cyber security is quite often sacrificed either for comfort or efficiency. The higher number of small and large-scale installations combined with easily exploitable vulnerabilities leads to a stronger exposure of building automation systems, which are often overlooked. Even worse, an adversary understanding the usage of regular building automation protocol functions for malicious purposes may not only create chaos within the breached building but can potentially even peek into internal, otherwise not reachable, networks through these building protocols.

This paper describes prototypic attack scenarios through building automation systems one should consider, and how even without exploits, a number of protocol functions in common building automation protocols like BACnet/IP and KNXnet/IP can support a malicious adversary going for those scenarios. The paper closes by discussing existing security measures proposed by the building automation industry as well as their adoption problems found in this field.

Keywords: building automation, BACnet, KNX, vulnerabilities, industrial control system, protocols

1. Overview of building automation protocols

Building automation is an integral part of all kinds of modern buildings and due to modernization efforts building automation is also added to existing or even old buildings. The interconnection of various types of building automation techniques allows, for example, to automatically trigger processes based on environmental values like time, temperature or humidity. Whether the heating is switched on early in the morning before the first employee arrives at work or the light is switched off after the last employee leaves the building – what can be done with building automation is only limited by the available controllable equipment and the desired optimization effect.

From an IT security point of view, it is especially interesting that in the field of building automation as well as in other automation areas the IP-compatible counterparts of KNX (KNXnet/IP) and BACnet (BACnet/IP) are used in addition to their conventional bus system version since these routable protocols significantly increase the attack surface of building automation systems.

[1] Limes Security GmbH
[2] FH St. Poelten

1.1. Importance and application areas of BACnet/IP and KNXnet/IP

BACnet/IP and KNXnet/IP are two open standards for building automation. The KNX protocols have been used for more than 20 years now and are supported by more than 300 manufacturers. The main application area is in home and building electronic systems for lighting and climate systems as well as security systems such as alarm systems. BACnet/IP, on the other hand, is a communication protocol specifically designed for the use in large installations. The scope of application for BACnet/IP is in building automation and control including fire detectors and surveillance or access control systems but is also used for the control and monitoring of elevators and escalators.

1.2. Logical structure

The components of building automation systems can be divided logically into three levels.

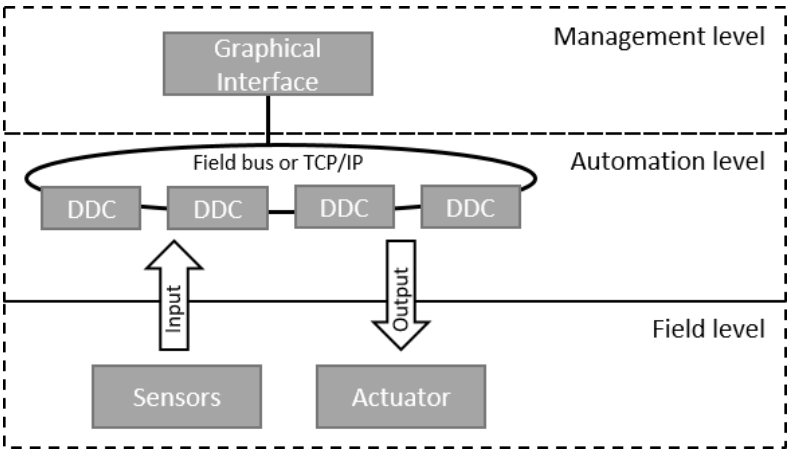

Fig. 1:Logical structure of building automation systems

The lowest layer, the field level, includes on the one hand sensors which are used to record analogue values and to transmit them to the layer above and on the other hand actuators such as valves or engines, which convert the obtained electrical signals into mechanical movements. In the middle layer, the automation level, there are so-called direct digital control devices (short DDCs) which can be used and programmed for control tasks within the building automation system. The management level is used for visualization, monitoring and operating or optimization of the building automation system. In addition, the management level can also be used as an access point for remote control functions.

However, due to the ever more rapid advances in the area of microprocessors, a distinct classification into the above-described levels is not always possible since the sensors and actuators get increasingly equipped with “intelligence” so that they can carry out the functionalities of the overlying levels. The increasing possibilities for interconnection of the various components through a wide range of different communication technologies ultimately contribute to the fact that the layers become more and more indistinct.

1.3. KNXnet/IP protocol 101

The KNX protocol can primarily be found in Europe and Asia, as it is the successor to former EIB. It was designed to be independent of the used hardware platform, and its main components are sensors, actuators and system devices, and components. KNX supports different transmission media, such as KNX TP (twisted pair), KNX RF (radio frequency) and of course for security purposes interesting KNXnet/IP (TCP/IP).

KNXnet/IP offers different groups of services: Core services for locating and identifying KNXnet/IP devices. Device management services for configuration purposes. Tunneling for point-to-point communication. Routing for runtime communication and finally remote diagnostic and configuration.

1.4. BACnet/IP protocol 101

BACnet was designed for communication between different building automation devices regardless of the manufacturers or service they perform and is favored in the US but can also be found in Europe.

The BACnet standard defines a set of various „objects “with a standard set of „properties “and services. The devices are not required to implement every service; however, some are mandatory such as the ReadProperty service.

As with KNX, BACnet can be implemented via various transmission media, again the occurrence as BACnet/IP on UDP port 47808 (0xBAC0) allows transmitting BACnet commands over IP networks.

From a security perspective, one group of dedicated services deserve special attention: The so-called BACnet/IP Broadcast Management Devices (BBMD) & Foreign Device Registration services. These allow an external BACnet/IP device to register itself as a foreign device as if it were part of the internal BACnet/IP network. For BACnet devices providing those functions and residing on the public internet, this means an attacker can access internal BACnet/IP devices even if they are not reachable directly via IP network, thereby effectively circumventing network access control.

As with KNX, BACnet/IP offers various services which may or may not be implemented fully, organized into the following groups of services: Alarm and event services for monitoring objects and receiving notifications. File access services for reading and writing files in BACnet devices. Object access services for reading/writing/modifying properties and adding/deleting objects. There are also remote device management services for special message transfer, addressing and auto-configuring. Finally, virtual terminal service which is a text-based connection to an application program on a remote device.

1.5. Attacks on BACnet/IP and KNXnet/IP in reality

The interest of hackers in industrial control systems in general has increased rapidly since the detection of Stuxnet in 2010. Building automation systems have not been reviewed yet by researchers with the same level of scrutiny. Interest to explore security of specific sub sectors of industrial control systems has risen steadily over the last years, driven by the lack of security and the quite often-insecure deployment of those systems.

According to the system search engine Shodan[3] more than 12,000 BACnet/IP devices and 130 KNXnet/IP devices worldwide are directly accessible via the Internet or can be controlled from outside the company network.

The exposure of these systems, which is a direct result of the reduction of non-Ethernet based bus networks in exchange for their IP-based versions, combined with the easy exploitability of often unfixed known vulnerabilities make building automation systems a potential springboard for attackers to not only manipulate the building automation systems themselves but rather to advance into the corporate network.

2. Building control abuse cases and attack scenarios for BACnet/IP and KNXnet/IP

The aim of building automation systems is a gain of comfort as well as optimization of energy efficiency and physical security aspects. Simplified: at the occurrence of an event, e.g. the exceeding or shortfall of a threshold value or triggering of a sensor, a series of previously determined sequences is executed. In addition to already well-established automation systems for lighting and climate control, functions from the fields of energy technology, security technology are now used as deployment scenario for building automation. The following section briefly presents possible applications from different areas of building automation with the goal to describe a concrete and realistic starting point for each area, which is then used as the target for an attack scenario.

2.1. Lighting

2.1.1. Starting point

The starting point for this use case is a building in which apartments, offices and seminar rooms are rented. In the stairwell of the corridor, motion detectors are installed, which trigger the lighting on the respective floor for a defined period. A network was set up in the entire building, which for economic reasons is also used for providing the guest WLAN for corporate customers and seminar visitors. In order

[3] Search engine for devices, accessible via the Internet. (https://www.shodan.io/)

to prevent configuration changes for lights and sensors from being made, the devices have been protected with a BCU password. At floors which are commercially used, video cameras were installed to monitor the glass door entrance. However, these come from the companies themselves and are therefore not accessible via the building automation network.

2.1.2. Attack scenario

The goal of the attacker in this scenario is to intrude into one of the offices undetected by the video camera. In the first step, the attacker has to gain access to the guest WLAN by retrieving the WLAN key. Once the attacker is connected to the guest WLAN, he can search for KNXnet/IP components either with the KNX software itself or, for example, a *nmap*[4]- script to get insight into the infrastructure. It would then be possible to send a command at regular intervals to switch off all lights, but this variant is too unreliable for the attacker due to possible latencies in the network. Therefore, he or she decides to change the configuration of the device so that all motion sensors send the power-on commands to the same light on the top floor. However, since the devices are protected by a password, the attacker must first guess the BCU key consisting of eight hexadecimal characters. He or she can then read the current configuration and make changes using a *Device Configuration Request* and the correct key. If the KNXnet/IP devices have been reprogrammed, the attacker can break open the glass door to the offices without activating the lighting and thus undetected from the video cameras.

2.2. Ventilating and air-conditioning technology: shading, ventilation, heating

2.2.1. Starting position

The setup for this use case is a modern single-family home made of many glass fronts with intelligent shading and interconnected heating and air-conditioning. The controllable blinds are used to prevent the rapid warming of the room, by lowering them at high outside temperatures. Air conditioning is only used throughout the day if the room temperature rises above a certain threshold in order to prevent damage to food, plants, and electronic appliances. The KNXnet/IP control system can be accessed from the outside via smartphone app to ensure that the rooms have reached a comfortable residence temperature at the return of the inhabitants. In addition to the controller, a web interface accessible from the Internet is offered by default, which is not used by the residents and has therefore not been configured and secured.

[4] Nmap (Network mapper, https://nmap.org/) ist einer der am weitesten verbreitete Network-Scanner

2.2.2. Attack scenario

Since the web interface for this KNX installation is accessible from the Internet, an attacker can find it when searching for KNX-specific content (website title, ports, text elements) or also via system search engines such as Shodan. In addition, the controller is not secured, which is why an attacker can abuse it immediately to make changes to the settings without having to enter the home network or to touch a device. This allows even a slightly skilled attacker to open the slats of the roller shutters on a hot day and for example, instead of cooling with the air conditioning, to turn on the heating system to increase the room temperature to an intolerable level or to overheat running electronic devices. On top of everything, a skilled attacker could blackmail the householder by changing the configuration of the control or block the accesses.

3. Protocol-level misuse of BACnet/IP and KNXnet/IP protocol functions

This section summarizes protocol functions of BACnet/IP and KNXnet/IP which may come in handy security-wise for an attacker. For a deeper insight into protocol specific attacks, please refer to the bibliography.

3.1. Protocol-level misuse of features and services of BACnet/IP

3.1.1. Initialize-Routing-Table

Routing tables allow an attacker to gain valuable information about the architecture and structure of the network of the building automation system. Sending an *Initialize-Routing-Table Request* without IP or port to a BACnet router leads to an answer with information about networks reachable via the targeted router.

3.1.2. Register-Foreign-Device

The *Register-Foreign-Device* service can be used to connect a foreign device, not located on the same internal network, via a BACnet router to another BACnet network. This service can be misused by an attacker to gain access to an internal building automation network although he is located outside of it, e.g. on the Internet).

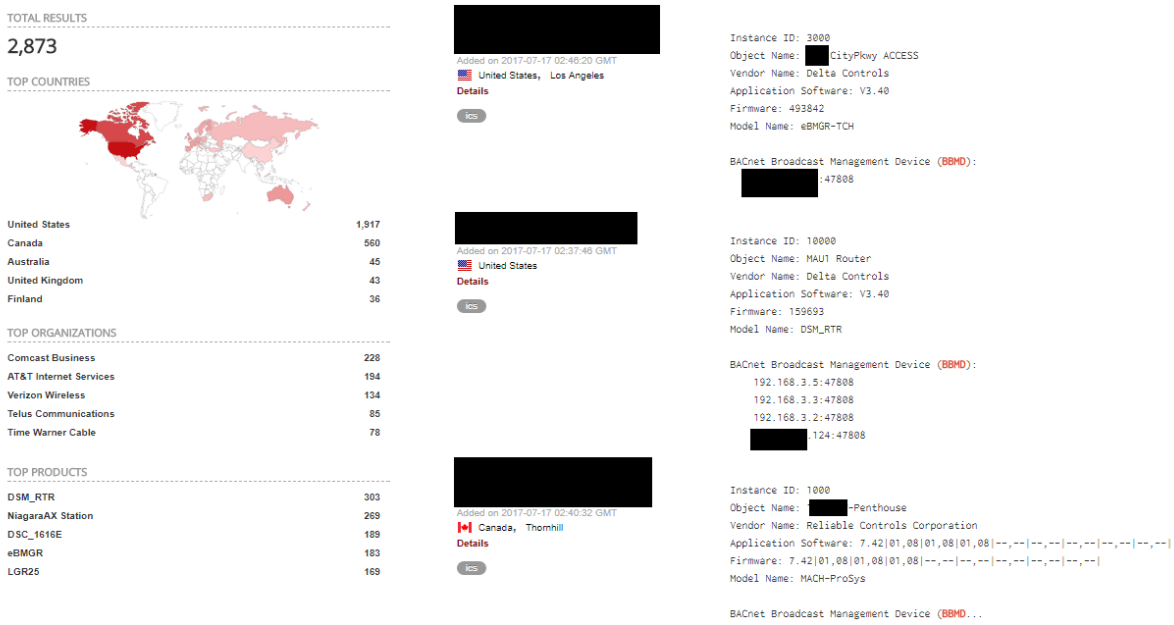

Figure 1Shodan showing nearly 2900 internet-exposed BACnet/IP systems which provide BBMD functions

3.1.3. I-Am-Router-To-Network

An *I-Am-Router-To-Network* message can be used to route messages between specific IPs over the sender. An attacker can use this service for a man-in-the-middle attack to gain insight into the content of the transmitted messages.

3.1.4. Router-Busy-To-Network

The *Router-Busy-To-Network* message is usually used by routers to tell other routers that certain networks are (temporarily) unavailable. The receiving device does not forward packets to the target network specified in the message for 30 seconds after receiving it. An attacker can use this functionality to periodically send a message with the source address of a targeted router to prevent communication on a network.

3.1.5. Read-/Write-Property

With the access to an automation network, the values of BACnet devices can be read out by the *Read-Property* or changed by the *Write-Property* command. An attacker can make use of this functionality and thus can control any system components or trigger events by changing the suitable values.

3.2. Protocol-level misuse of features and services of KNXnet/IP

3.2.1. SEARCH_REQUEST

If a SEARCH_REQUEST is sent within a network of KNX devices, the sender receives a response from all available KNX servers. These KNX servers are the interfaces to terminal devices like light bulbs or switches.

3.2.2. ROUTING_INDICATION

The ROUTING_INDICATION flag indicates a KNX server that the included KNX message should be transmitted via KNXnet/IP to the address given in the header of the message. The body of the KNXnet/IP message contains the payload for the terminal device – for example a new status like "0 – light off".

3.2.3. DEVICE_CONFIGURATION_REQUEST

Using a DEVICE_CONFIGURATION_REQUEST, the configuration of a KNX device can be read out or changed. The configuration can be protected from unauthorized modification by a so-called BCU key. The BCU key consists of eight hexadecimal characters (default 0xFFFFFFFF) and can be guessed in a reasonable amount of time by trying out all possibilities.

4. Penetration testing tooling for building automation systems

This section gives a brief overview of software tools which the authors have found handy during conduction of penetration tests of building automation control systems.

4.1. Discovering building automation systems

Luckily enough for penetration testers, for some of the platforms and protocols used in building automation control systems, some tooling exists already or was created rather recently.

Through making use of the nmap scripting engine (NSE), some of the necessary protocols come already as part of the NSE scripts pre-packaged with nmap [1]. These include for instance discovery scripts for the KNXnet/IP protocols as well as BACnet/IP and the more generic Modbus-TCP protocol that is also found in building automation control.

Another option for extending nmap are the NSEs published by Digitalbond through their project Redpoint [2], also targeting BACnet/IP as well as Modbus TCP for device enumeration.

Robbie Corley created the project HVACscanner [3], which isn't looking for specific building automation control protocols, but locates Honeywell/Tridium/Niagara HVAC JACEs/Controllers through the method of detecting matching HTTP fingerprint/strings.

Finally, Tenable's Nessus vulnerability scanner [4] also is able to detect a certain number of technologies for building automation systems; most noteworthy are again BACnet/IP as well as Modbus TCP protocol detection and OPC server detection.

For interpreting actual BACnet/IP or KNXnet/IP datagrams and packet captures, Wireshark provides already dissectors for those protocols.

4.2. Security tooling specific for KNXnet/IP

As with other industrial control system protocols, the engineering software for programming and engineering KNX systems has certain functions that come in handy for security purposes as well.

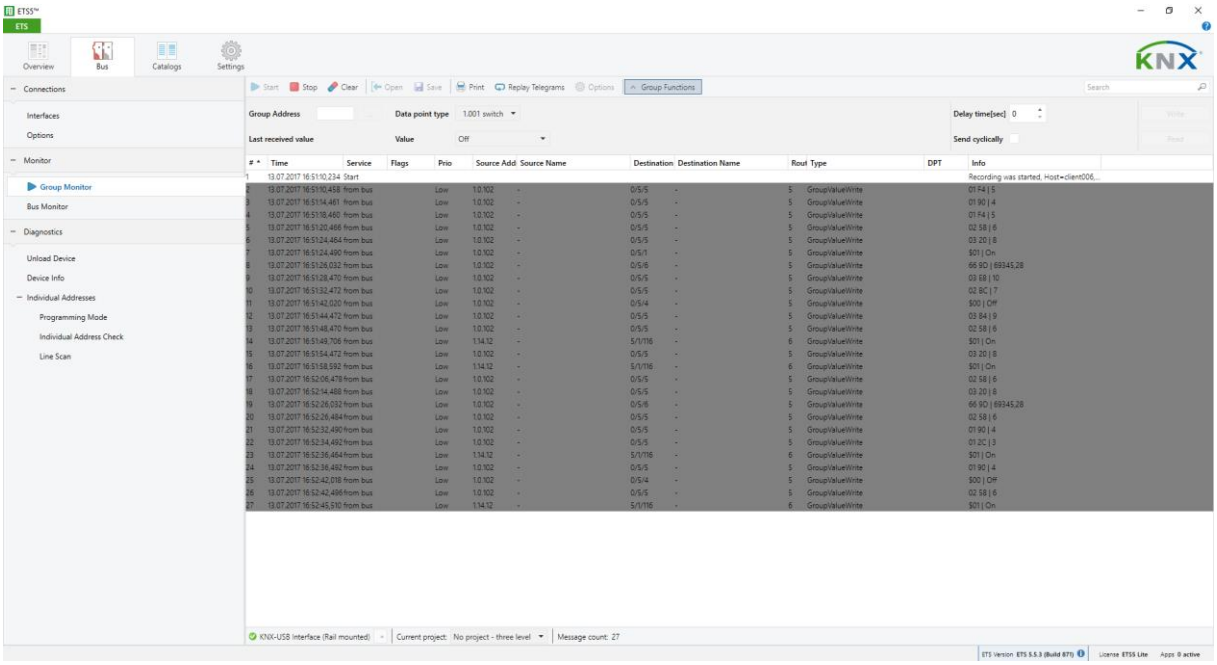

Figure 2KNX ETS showing capability of bus monitoring in order to learn the applied logic adressing scheme

The screenshot above shows ETS's capability for listening to KNX messages, thereby allowing to learn the logic addressing scheme used by its builder. It even allows already replaying of specific KNX messages.
Another security-wise interesting function of ETS is the possibility of doing a so-called "line-scan" which allows scanning for active devices within a specific address group KNX-wise, comparable to scanning e.g. for devices in a specific subnet IP-wise.

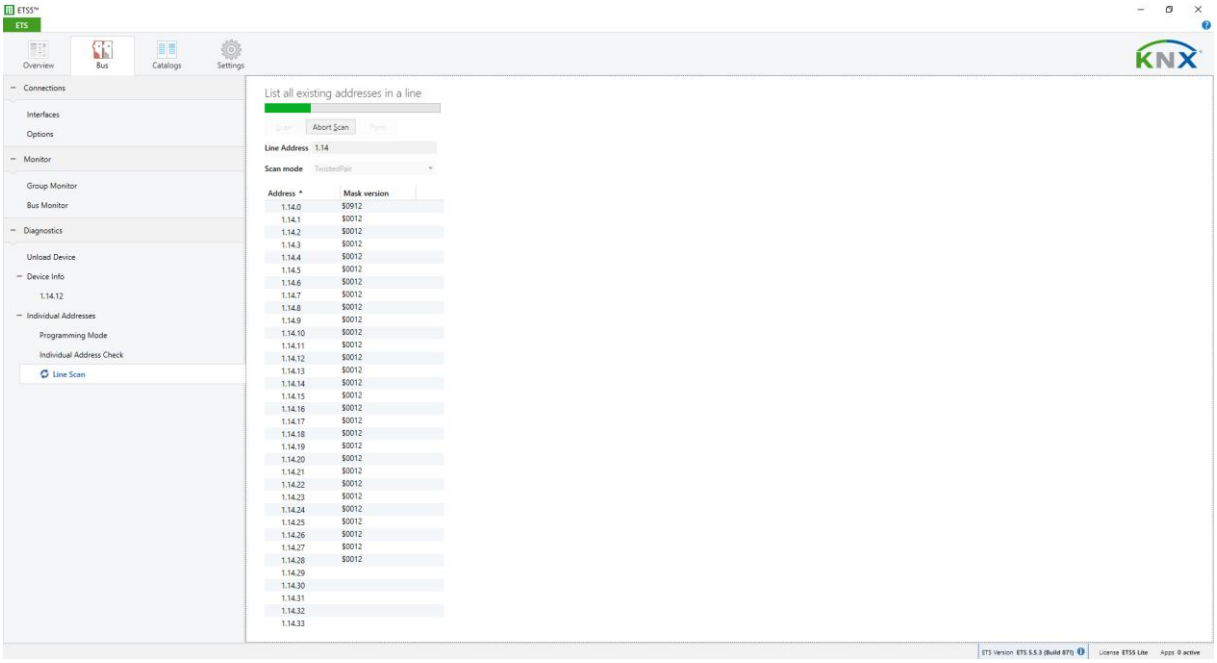

Figure 3 KNX ETS revealing active devices during a line scan

Finally, there is the KNXmap [5] tool implementing many security-relevant functions that may come in handy during a security test: For scanning purposes, KNXmap assists in identifying KNX gateways via unicast discovery messages (default scan mode). It also scans for bus devices attached to KNX gateways (with optional device fingerprinting). Searching for KNX gateways is supported via multicast messages (with --search).
KNXmap also provides bus monitoring functions like the one ETS has. Here, it reads debug communication on the bus and allows for passive information gathering (i.e. for motion sensors.

4.3. Security tooling specific for BACnet/IP

Two free tools be can be recommended for exploring BACnet/IP: BACnet Tools [6] (BACnet protocol stack) as well as Yabe [7] (Yet another BACnet explorer).
BACnet Tools is especially interesting for pentesting purposes as it provides most components of a BACnet system such as e.g. a BACnet/IP server and a BACnet/IP client as command line tools which is ideal for scripting.
Most of the security-relevant BACnet/IP commands referenced in section 3.1 such as Read-/Write-Property or Register-Foreign-Device are supported by one or both tools.

5. Summary of existing building automation control security recommendations

As with many other industrial control system protocols, neither BACnet nor KNX have specified strong native security measures in the original standards. As regular ICS, building automation control started as proprietary protocols and closed systems. Over time the technology shifted to standardized bus protocols and serial lines, finally arriving today where those protocols are transmitted with open protocols such as Ethernet and IP.

As the standardization organizations behind certain building automation protocols began to recognize security threats, they created several extensions and recommendations for improving and retro-fitting security with BACnet/IP and KNXnet/IP systems, trying to compensate their lack of certain native security capabilities. Those recommendations are summarized in the following sections.

5.1. Security recommendations for BACnet/IP

In 2006 already, a proposal for a security add-on for the BACnet standard was published by the American Society of Heating, Refrigerating And Air-Conditioning Engineers (ASHRAE), which extensively describes mechanisms for the network-based protection of BACnet. [10] The main points of this supplement, as well as other recommended security measures, are dealt with in the following section.

5.1.1. Physical isolation

As a first step, rooms containing building automation devices should only be accessible to authorized persons. Furthermore, the devices should be permanently

built-in and installed, so that simple or unnoticed replacement is not easily possible. The building automation network should also be operated separately from other networks and should be operated with its own network infrastructure devices.

5.1.2. Secure external access

The router used for the building automation system maintenance should not have open, unprotected ports such as http in the direction of the Internet or other external networks. If access from an external network is required, a firewall should be configured as access protection, and a VPN for remote access should be set up.

5.1.3. Implementation of network security architecture

In the security enhancement of the standard, mechanisms are proposed whereby BACnet can be extended with authentication, integrity protection, and confidentiality. The use of S*hared Keys* allows both devices and users to be authenticated and using S*ecure Messages* integrity, confidentiality, and protection against replay attacks is ensured. Secure Messages ensures that the messages that are otherwise sent in plain text are "packaged" in a secure container, which is then either signed and/or encrypted according to the security level. Replay protection can be ensured by adding a time stamp and a message ID.

5.1.4. Use of security proxies

A so-called *Security Proxy* was defined by ASHRAE to protect devices that do not support security mechanisms as standard. A *Security Proxy* is a secure router, which uses security mechanisms on behalf of the devices located behind. Which measures and to which extent to which messages are to be used must be individually configured for each router. In addition, such a security proxy can use filter rules to ensure for example messages with invalid signatures or incorrect authentication information to be discarded.

5.2. Security recommendations for KNXnet/IP

As with BACnet, no native security mechanisms have been implemented in the KNX protocol, which is why the operators or integrators themselves must take measures to retrofit security and thereby limit the attack points in KNX installations as much as possible. In the year 2015, the KNX Association published a position paper on KNX security, which is intended to serve as a guideline for improving security and is described here in the most important points. [8]

5.2.1. Physical isolation

See section 5.1.1

5.2.2. Secure external access

See section 5.1.2

5.2.3. Restrict communication channels

In order to restrict unwanted or potentially dangerous communication, the KNX Association recommends not forwarding messages with incorrect source addresses and not allowing point-to-point connections and broadcast messages via the router of a KNX area. In order to additionally prevent an external KNX device from accessing the communication of the entire KNX system, a line coupler with a filter table should be used per area which blocks group addresses that are not linked to that area.

5.2.4. Secure coupling with other systems

If KNX devices are coupled with security-relevant systems such as alarm systems or hazard reporting systems, attention should be given to the recommendation that these are not located on the same network, but rather communicate with each other via separate interfaces or potential-free contacts (binary and analogue inputs) in order to prevent the attack of an invader.

5.2.5. Secure configuration

The application software from KNX (ETS) allows the assignment of a project-specific password (BAU / BCU key), which prevents the device configuration from being read and changed. Although the password, consisting of eight hexadecimal characters, can be guessed by a brute force attack, it is a further obstacle for a potential attacker.

5.2.6. Secure communication

To protect the communication between KNX devices during runtime, KNX introduced two security enhancements: KNX IP Secure and KNX Data Security. These extensions allow the establishment of a secure connection between KNX devices and enable authentication, encryption and replay protection. However, the security enhancement can only be used from ETS 5.5.

6. Trends and outlook

It is quite likely that attackers will increasingly recognize the benefits of hacking building automation systems.

Especially nation-state adversaries, contract hackers, and terrorists may have an interest in taking over and manipulating building automation control systems, e.g. for creating panic or to support physical access operations.

In particular, the increased integration of building automation with other IP networks by KNXnet/IP and BACnet/IP leads to new access possibilities, which leads to greater risks if the rather poor native security capabilities of building automation systems are not compensated through other controls.

While the context of building automation systems has already served as an entry gate for high-profile incidents in the past e.g. in the widely known hack against TARGET [9], it is to be assumed that building automation itself will be more of a core target in the future.

A short survey finally carried out among European system integrators, and users of building automation showed the urgent need for system integrators to catch up with understanding security risks. The survey showed that only a rather small minority of interviewed system builders had actually stepped out of their original electrical engineering field and started to think about including security at all.

Unless both technology and the security mindset of system integrators change for the better, we will continue to have insecurely deployed building automation control systems and thereby insecure buildings.

Sources

[1] "nmap NSE script repository on github," [Online]. Available: https://github.com/nmap/nmap/tree/master/scripts. [Accessed 15 07 2017].

[2] Digitalbond, "Project Redpoint, Digital Bond's ICS Enumeration Tools," [Online]. Available: https://github.com/digitalbond/Redpoint. [Accessed 10 07 2017].

[3] R. Corley, "HVACScanner github project pake," [Online]. Available: https://github.com/musicmancorley/HVACScanner. [Accessed 12 07 2017].

[4] "Tenable Nessus Plugins," Tenable Security, [Online]. Available: https://www.tenable.com/plugins/index.php. [Accessed 10 07 2017].

[5] takeshixx, "KNXmap Github project page," [Online]. Available: https://github.com/takeshixx/knxmap/) . [Accessed 10 07 2017].

[6] S. Karg, "BACnet protocol stack on Sourceforge," [Online]. Available: https://sourceforge.net/projects/bacnet/files/bacnet-tools/. [Accessed 11 07 2017].

[7] F. Chaxel, M. Kvistgaard, A. Guzik, C. Günther and T. Al-Salek, "Yet Another Bacnet Explorer project page on Sourceforge," [Online]. Available: https://sourceforge.net/projects/yetanotherbacnetexplorer/. [Accessed 12 07 2017].

[8] KNX Association, "KNX," 2015. [Online]. Available: https://www.knx.org/media/docs/downloads/Marketing/Flyers/KNX-Secure-Position-Paper/KNX-Secure-Position-Paper_de.pdf. [Accessed 28 1 2017].

[9] B. Krebs, "Krebs on Security, Target Hackers Broke in Via HVAC Company," Februar 2014. [Online]. Available: https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/.

[10] S. Heinle, Heimautomation mit KNX, DALI, 1-Wire und Co., Bonn: Rheinwerk

Verlag, 2016.

[11] J. Thoma, "golem.de," 24 3 2015. [Online]. Available: http://www.golem.de/news/knx-schwachstellen-spielen-mit-den-lichtern-der-anderen-1503-113085.html. [Accessed 25 1 2017].

[12] D. Goodin, "The Register," 1 7 2009. [Online]. Available: https://www.theregister.co.uk/2009/07/01/hospital_hacker_arrested/. [Accessed 25 1 2017].

[13] M. Fuchssteiner, "BACnet Protocol Security and Attacks," Fachhochschule St. Pölten, St. Pölten, 2014.

[14] R. Seyer, "Penetration Testing of KNXnet/IP," Fachhochschule St. Pölten, St. Pölten, 2016.

[15] IMU Institut, "Aufzugs- und Fahrtreppenbranche in Deutschland - Entwicklungstrends und Herausforderungen," IMU Institut, Stuttgart, 2015.

[16] H. Wirth, "Aktuelle Fakten zur Photovoltaik in Deutschland," Fraunhofer ISE, Freiburg, 2017.

[17] Statistika - Das Statistik-Portal, "Fakten zum Thema: Photovoltaik in Deutschland," [Online]. Available: https://de.statista.com/themen/156/photovoltaik/. [Accessed 26 1 2017].

[18] R. Nestler, "Der Tagesspiegel," 17 3 2015. [Online]. Available: http://www.tagesspiegel.de/wissen/sonnenfinsternis-2015-uebersteht-das-stromnetz-die-dunkelheit/11502988.html. [Accessed 27 1 2017].

[19] Bundesnetzagentur, "Strom-Report.de," 2015. [Online]. Available: http://strom-report.de/photovoltaik/#photovoltaik-stromerzeugung. [Accessed 27 1 2017].

[20] A. Rossmann, Strukturbildung und Simulation technischer Systeme (Band 2/7), Berlin: epubli GmbH, 2014.

[21] ASHRAE, "ASHRAE BACnet," 3 2006. [Online]. Available: http://www.bacnet.org/Addenda/Add-2004-135g-PR1.pdf. [Accessed 29 1 2017].