Identifying unsecured building automation installations

Friedrich Praus
University of Applied Sciences Technikum Wien
Department of Embedded Systems
praus@technikum-wien.at

Wolfgang Kastner
Vienna University of Technology
Automation Systems Group
k@auto.tuwien.ac.at

Abstract

Building automation systems rely more and more on IP-based communication, which allows easier management, maintenance and, in general, interaction with other domains. When the connection to the Internet comes into play, security mechanisms need to be deployed to prevent attacks on these systems. Based on a worldwide scan of IPv4 addresses, this paper illustrates that security awareness is unfortunately still neglected. Thousands of building automation systems are directly connected to the Internet, allowing unauthenticated and unauthorized access to their underlying datapoints.

1. Introduction and motivation

Building automation systems (BAS) improve comfort, control and maintenance in smart homes and buildings. Following the major trend, standardized, open and well established technologies such as BACnet, EnOcean, KNX, LonWorks, Modbus are widely used. Similar to the Industry 4.0 initiative in the industrial automation or the establishment of cyber-physical systems, Ethernet and IP-based interconnection using specific interconnection devices (ICDs) (e.g. routers, gateways) are getting increasingly important since an integration and connection to the management level is achieved in a more convenient way. Remote access paves the way for energy management systems dedicated for functional buildings and ambient assisted living applications tailored to our homes of which future solutions may even reside within the cloud.

The Internet itself, however, is an open medium, which is used by adversaries all over the world to attack connected devices – including automation technologies. In the industrial automation, such attacks already have been performed (e.g. Stuxnet [5]). Security awareness among integrators, developers and end-users, however, is still missing as recent research and experiments have shown (e.g. Industrial Risk Assessment Map (IRAM) [8]). Thousands of SCADA and industrial control systems are directly connected to the Internet exposing them to attacks.

Even worse, often security vulnerabilities are present in those sensors, actuators and controllers (SACs). Early 2013, a software bug in a block heat and power plant has been discovered, which allowed unauthorized remote control. Meanwhile, the software has been fixed and a VPN box is available for secure data exchange [3]. Beginning of May 2013, a software bug in a widespread industrial control system has been discovered, which also allowed unauthorized remote control. 500 installations in Germany were affected [2]. It lasted till August 2013 until the manufacturer released an update for up to 200.000 worldwide installations [7].

Recent research and analyses targeted industrial automation mainly based on the fact, that a web-server has been running on the default TCP port 80 of affected SACs which has been exposed to the Internet search engine Shodan (`http://www.shodanhq.com/`). To our best knowledge, up to now no extensive research is available, which deeply analyzes BASs being connected to the Internet.

Therefore, this work in progress is dedicated to IP security of existing (and installed) BASs. In Section 2, the open BASs BACnet and KNX and the basic technology required to connect them to IP-based networks are briefly described. It is also outlined how discovery is standardized. Section 3 describes a scanning architecture to detect BASs being connected to the Internet and presents the results of a worldwide IPv4 scan. Finally, Section 4 outlines the future work with ongoing scans for installations using other BAS standards (e.g. EnOcean, LonWorks, Modbus).

2. BACnet/IP and KNXnet/IP

Building Automation and Control networking protocol (BACnet) [1] provides the network option BACnet/IP, which permits BACnet devices to use standard Internet Protocols (UDP and IP) as virtual data link layer.

BACnet defines the network visible part called BACnet object of a single data element. The internal data structure is not covered. Each BACnet object has a dedicated object type and represents a collection of properties. Each property has a data type defining the size and encoding of the data element. An object in a network is referenced by its system-wide unique `Object_Identifier` property, which usually is assigned during configuration. This provides a mechanism for accessing every object in the

2014 IEEE Emerging Technology and Factory Automation (ETFA)
978-1-4799-4845-1/14/$31.00 ©2014 IEEE

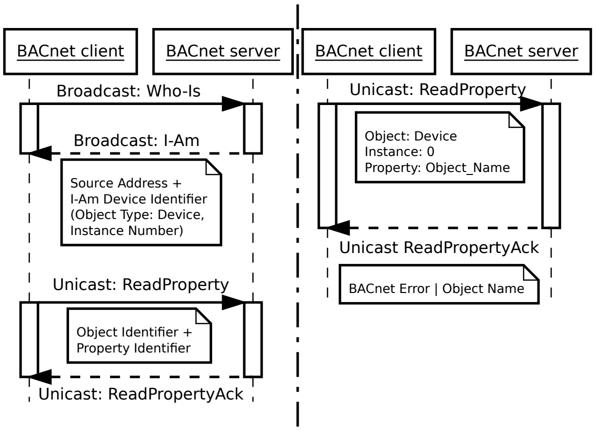
BACnet client
BACnet server
BACnet client
BACnet server
Broadcast: Who-Is
Broadcast: I-Am
Source Address + I-Am Device Identifier (Object Type: Device, Instance Number)
Unicast: ReadProperty
Object Identifier + Property Identifier
Unicast: ReadPropertyAck
Unicast: ReadProperty
Object: Device Instance: 0 Property: Object_Name
Unicast ReadPropertyAck
BACnet Error | Object Name

Figure 1. BACnet communication

control system network via defined object access services.

The left part of Figure 1 shows an example communication. To search for BACnet devices in a network, the `Who-Is` broadcast service can be used by BACnet clients. Each receiving BACnet device shall respond with a broadcast `I-Am` request containing the `IAmDeviceIdentifier` (object type, device instance number) and some further properties. The most important services used to access and manipulate objects are `ReadProperty` (to read the value of a property), and `WriteProperty` (to set a new property value), which are sent using unicast communication and the object and property identifier.

BACnet integrates protocol security extensions for quite some time (since Addendum g in 2008), which should protect the exchanged data against interception, modification, and fabrication. Furthermore, advanced security concepts like the use of different key types and key revisions have been introduced.

KNXnet/IP describes transportation of KNX telegrams on top of IP networks with main purpose to expand building control beyond the local KNX bus. KNXnet/IP supports discovery and self-description of a KNXnet/IP server using one well known discovery endpoint. A server should at least support one control endpoint and one data endpoint (UDP or TCP on arbitrary ports) per KNX connection for additional communication.

The left part of Figure 2 shows an example communication. For discovery of a KNXnet/IP server, the client sends a `SEARCH_REQUEST` to the discovery endpoint (system setup multicast address 224.0.23.12, UDP port 3671). Every server receiving the request should respond immediately with a `SEARCH_RESPONSE` frame for each of its service containers containing the Host Protocol Address Information (HPAI) (IPv4: IP address and port number) of the control endpoint. Afterwards, the client typically sends a `DESCRIPTION_REQUEST` to all received control endpoints using unicast telegrams and the information contained in the HPAI. Servers respond with a `DESCRIPTION_RESPONSE`, containing Description Information Blocks (DIBs) with supported protocol, capabilities, state information and an optional friendly name. To connect to the control endpoints, a unicast `CONNECT_REQUEST` can be used.

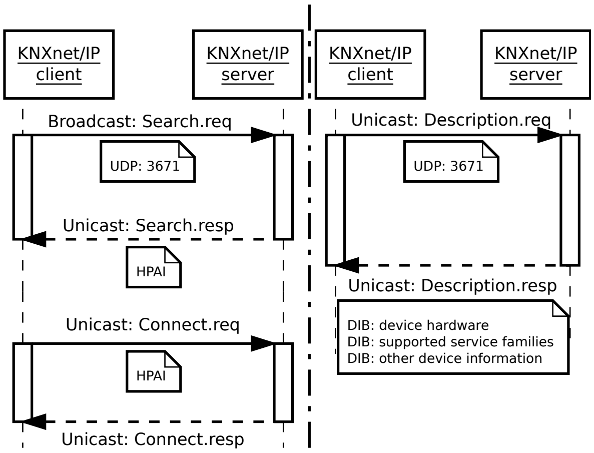

Figure 2. KNXnet/IP communication

Recently, the security extension KNXnet/IP Secure [6] providing data integrity, freshness, confidentiality and mutual authentication has been standardized. However, some limitations concerning the provided level of security have already been addressed in [4].

3. A survey on world-wide installations

3.1. Attack vector

The goal of this WiP is to research whether and how many BASs installations based on BACnet and KNX are being connected to the Internet and what security measures are currently implemented. The following assumptions are made to find such sites:

- BACnet devices are connected to the Internet using their BACnet/IP network interface or using BACnet/IP ICDs (i.e. BACnet IP routers/gateways).
- KNX installations are connected to the Internet using KNXnet/IP ICDs. KNX devices directly connected to an IP backbone ("native" KNX IP devices) are not considered in this work.
- IPv4 is used, no distinction between dynamic or static IP address ranges is taken.
- The installations are standard compliant as described in Section 2 and are reachable via the default ports. Devices are either being directly connected to the Internet using a public IP address or reachable using port forwarding to a private IP address. These ports are not filtered using a firewall.

Based on these assumptions, the following attack vector can be used to analyze BASs being openly connected to the Internet.

Iterate through all (worldwide) IPv4 addresses and try to discover BACnet or KNX services. Simple port scans using common tools (e.g. nmap) cannot reveal BAS specific details (e.g. human readable names, manufacturers) of connected installations and false positives might occur if non BAS protocols rely on this port. Also such port scans without deeper protocol knowledge might result in false negatives, since a connected device simply might ignore such scans.

As shown in Section 2, the discovery mechanisms of BACnet and KNX rely on broadcasts/multicasts. Within the Internet, however, UDP/IPv4 multicast and broadcast telegrams and TCP/IPv4 broadcast telegrams are not routed, and TCP/IPv4 multicast telegrams are not supported. Thus, discovery does not work for non local networks. Trying to perform a (slightly not standard compliant) discovery using unicast telegrams from the client to the server might work in this direction, but according to the specifications servers might reply using multicast/broadcast telegrams which will not arrive at the client.

To discover BACnet/IP based installations a request as shown in the right part of Figure 1 can be used. This is handled by issuing a well formed and standard compliant unicast (UDP/IP, port 0xBAC0) `ReadProperty` on property `Object_Name` to a probably existing `Device Object, Instance 0` and evaluating the unicast `ReadPropertyAck`. If a BACnet server is connected, it either will reply with a BACnet error if for example the object is not found, or with the proper `Object_Name`.

The only well known default port in KNXnet/IP is the control endpoint UDP 3671, which can be used to get information about the data endpoint. The KNX standard defines, that devices may use the same port numbers for both endpoints but may also assign different port numbers for data exchange. Out of the box experiments with ICDs of the major KNX manufacturers revealed that control and data exchange is implemented using equal ports. Hence, to discover KNXnet/IP based installations, a request as shown in the right part of Figure 2 can be used. A well formed and standard compliant unicast `DESCRIPTION_REQUEST` is sent to the data endpoint, which is assumed to be located on UDP port 3671. If a KNXnet/IP ICD is connected, it replies with a unicast `DESCRIPTION_RESPONSE` containing the DIBs.

If the IP address of a BAS installation is found, further investigations can be done:

- Perform a detailed port scan on all ports. Often services, such as web servers, visualizations or webcams are also reachable via the same IP address on probably non standard ports. Additional information regarding the BAS installation (e.g. human readable installation name or abbreviation, manufacturer of the connected device) can easily be gained by simply accessing these services. If authentication is requested, supplying no password, default usernames and passwords gained out of the user manual of the specific manufacturer or trying guest accounts might give access.
- Perform geolocation and "whois" DNS lookups of the IP address. Information such as country, city, organization, Internet service provider, latitude and longitude can simply be gained. Thus it might be possible to clearly identify a BAS installation.
- If a BACnet/IP installation is found `Read` and `Write Property` requests on different object types or object identifiers can be tried.
- If a KNXnet/IP installation is discovered, connecting to the installation via a KNXnet/IP tunneling request can be tried. It is then possible to read and write group addresses or receive all KNX data of the BAS.

3.2. Scanning architecture

A simple but modular scanning architecture, which allows to deeply analyze BASs being connected to the Internet has been developed. A multi-threaded C-program initializes logging facilities, handles inter-process communication and synchronization using semaphores and allows to limit the amount of parallel IP connections. Pluggable protocol stacks (BACnet: `http://sf.net/projects/bacnet/` ,version 0.8.2; KNX: `http://www.auto.tuwien.ac.at/~mkoegler/index.php/bcusdk`, version 0.0.5) provide the communication services.

The test system has been connected to the Internet using a consumer service provider with bandwidth 150Mbit/s download and 15Mbit/s upload. System specifications are an Intel Atom CPU 330 (2 cores, 1,6GHz) and 3GB RAM. The IP addresses 1-9.*.*.*, 11-126.*.*.*, 128-223.*.*.* have been scanned. Concurrent connections have been limited to 2048/second. The timeout per connection has been set to 3 seconds. Discovery started on 6th January 2014 and lasted till 9th May 2014. The average CPU load was around 19%, average memory usage about 400MB, average incoming traffic 50kBit/s and average outgoing traffic 532kBit/s. After scanning, IP geolocation information has been gathered using the Maxmind GeoLite Country and GeoLite City database (`http://dev.maxmind.com/geoip/legacy/geolite/`). The search for additional open ports has been performed using nmap and TCP SYN scans. The final visualization is based on Google Earth.

3.3. Scan results

Table 1 shows the scan results grouped by technology and summed up per country. A total of 17259 BAS installations has been detected. BACnet is being widely used in the US and Canada whereas KNX is very popular in Europe. The installations ranged from business parks and towers, high schools, shopping plazas, water pollution control stations, fire stations, churces to smart homes with control of private saunas. Figure 3 shows the geolocations of the installations in Europe.

A deeper analysis of BACnet installations is shown in Table 2. Most of the responses correspond to installations where no `Device Object` with `Instance` 0 is found. Since more detailed scans (with e.g. different instance numbers) on these installations can be considered as illegal, they have been left out of scope. A possible real adversary, however, will not stop at this point. In 250 cases, it was possible to read out the object name. Only in 3 cases

Country	BACnet	Country	KNX
US, United States	8989	DE, Germany	627
CA, Canada	2296	NL, Netherlands	522
FI, Finland	282	ES, Spain	332
AU, Australia	271	FR, France	244
ES, Spain	231	AT, Austria	220
FR, France	148	CH, Switzerland	204
SE, Sweden	138	IT, Italy	173
GB, United Kingdom	131	NO, Norway	129
DE, Germany	118	SE, Sweden	120
KR, Korea, Republic of	110	BE, Belgium	119
NO, Norway	103	IL, Israel	109
IT, Italy	101	PL, Poland	67
CZ, Czech Republic	98	GB, United Kingdom	56
TW, Taiwan	97	GR, Greece	42
NL, Netherlands	89	CZ, Czech Republic	30
NZ, New Zealand	47	RU, Russian Federation	24
HK, Hong Kong	45	VN, Vietnam	23
JP, Japan	44	TR, Turkey	21
AT, Austria	42	LT, Lithuania	20
CH, Switzerland	39	PT, Portugal	20
worldwide	13964	worldwide	3295

Table 1. Scan results (top 20 countries)

Return value (E)rror, (R)eject, (A)bort	Count
E: object: unknown-object	13297
Empty	333
Success	250
E: device: unknown-object	31
R: Unrecognized Service	28
E: device: other	5
device	3
E: object: unsupported-object-type	3
E: property: unknown-object	3
E: services: service-request-denied	2
A: Buffer Overflow	2
E: device: configuration-in-progress	2
E: object: other	2
A: Other	1
A: Preempted by Higher Priority Task	1
E: object: service-request-denied	1

Table 2. BACnet responses

Port	Count
80/http	7846
443/https	3472
135/msrpc	3302
139/netbios-ssn	3268
445/microsoft-ds	3261
8080/http-proxy	2504
21/ftp	2375
3389/ms-wbt-server	1983
23/telnet	1874
3011/trusted-web	1861
5960/unknown	1524
22/ssh	1451
25/smtp	1297
1723/pptp	1163
50001/unknown	1086

Table 3. Open ports

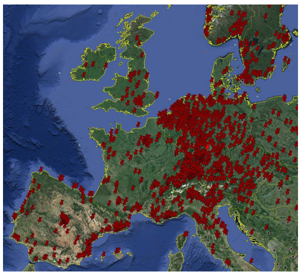

Figure 3. BAS geolocations

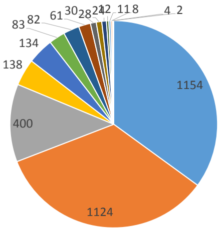

Figure 4. KNX device manufacturers

(2x `services: service request denied`, 1x `object: service request denied`) the request has been denied which shows, that BACnet security as standardized since 2008 is seldom enabled in real life.

A total of 3.295 KNX installations have been detected. The MAC addresses have been extracted out of the DIBs and its `Organizationally Unique Identifiers` have been used to to find out the vendors of the devices. Devices per vendor have been summed up. Figure 4 shows this anonymized analysis. Under the assumption that the security awareness of people installing KNX based systems is independent of the devices they deploy, the following estimation holds: The percentage of total installations to directly connected BAS can be estimated if the number of sold devices of one manufacturer is known. Investigations revealed, that at least 1-5% of all KNX installations are being insecurely connected to the Internet.

Table 3 shows the additional top 15 open TCP ports grouped by port number. Typically, a web server is also available (especially in BACnet based installations) and authentication is required. Since either default or guest passwords often permitted a login, or a direct connection using the BACnet/IP or KNXnet/IP protocol is allowed anyway, severe security attacks cannot be prevented.

4. Work in Progress

By now the first results of this investigation show that security awareness in the BAS domain is still deeply missing. Thousands of BASs are being directly connected to the Internet and allow unauthenticated and unauthorized access. Only two BAS technologies have been analyzed, other relevant standards (e.g. EnOcean, LonWorks, Modbus) will be covered in ongoing work.

In order to enhance security in BASs, a comprehensive approach is needed: On the one hand technologies need to provide mechanisms for secure communication, secure software and update routines as well as protection to provide availability. On the other hand also education covering security mechanisms and accompanying measures are needed in the BAS domain. Immediately, mechanisms such as firewalls helping to prevent access and Virtual Private Networks (VPNs) allowing to connect remote sites need to be deployed in BASs.

References

[1] *BACnet - a data communication protocol for building automation and control networks*. ANSI/ASHRAE 135, 2012.

[2] heise Security. Kritische Schwachstelle in hunderten Industrieanlagen. online: http://heise.de/-1854385, May 2013.

[3] heise Security. Vaillant-Heizungen mit Sicherheits-Leck. online: http://heise.de/-1840919, Apr 2013.

[4] A. Judmayer, L. Krammer, and W. Kastner. On the security of security extensions for IP-based KNX networks. In *Proc. of the 10th IEEE International Workshop on Factory Communication Systems (WFCS 2014)*, May 2014.

[5] S. Karnouskos. Stuxnet worm impact on industrial cyber-physical system security. In *IECON 2011 - 37th Annual Conference on IEEE Industrial Electronics Society*, pages 4490–4494, 2011.

[6] KNX Association. *KNX System Specifications, version 2.1*. ISO/IEC 14543-3, Jan 2014.

[7] Louis-F. Stahl. Kritisches Sicherheitsupdate für 200.000 Industriesteuerungen. online: http://heise.de/-1934787, Aug 2013.

[8] SCADACS. Industrial Risk Assessment Map (IRAM). online: http://www.scadacs.org/iram.html, Aug 2013.