Spotting unsecured KNX installations

Friedrich Praus and Wolfgang Kastner

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

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

IP based KNX installations are meantime widespread all over the world. They allow interconnection of different KNX field segments to a common backbone which might be home for management applications. Also, IP-based access paves the way for energy monitoring and management systems dedicated for functional buildings. Future homes and ambient assisted living applications may benefit from new services that 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. In the industrial automation, such attacks already have been performed. Even worse, often security vulnerabilities are present in those sensors, actuators and controllers. To our best knowledge, up to now no extensive research is available, which deeply analyzes existing KNX installations being connected to the Internet.

Thus, based on a worldwide scan of IPv4 addresses, this paper will illustrate that security awareness among integrators, developers and end-users is unfortunately still neglected in the KNX domain. Thousands of installations are directly connected to the Internet, allowing unauthenticated and unauthorized access to their underlying datapoints. This paper also covers a discussion on possible countermeasures as well as the non-functional and functional security requirements in KNX.

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 or 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. Also, remote access paves the way for energy management systems dedicated for functional buildings and ambient assisted living applications tailored to our homes where 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 [6]). 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) [10]). 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 (Vaillant [4]). 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 [3]. It lasted till August 2013 until the manufacturer released an update for up to 200.000 world-wide installations [8].

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.

The paper is organized as follows: Section 2 describes KNXnet/IP and its mechanisms supporting discovery and self-description of a KNXnet/IP server. Section 3 outlines the attack vector being used to research whether and how KNX installations are being connected to the Internet and what security measures are currently being implemented. It further shows the scanning architecture (hardware and software), which allows to deeply analyze such installations. Finally the scan results are presented, demonstrating that more than 3000 KNX installations are being connected unsecured to the Internet. Section 4 concludes with a discussion on how attacks to KNX systems can be prevented. This section will also cover a short analysis of the KNX specification 2.1.

2 KNXnet/IP

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 (cf. Figure 1).

The left part of Figure 2 shows a more detailed 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.

Security of KNXnet/IP has been neglected in the beginning. It was considered out of scope and relied on security by obscurity. The current KNXnet/IP specification [7, 03_08_01 Overview v1.4 p. 11] describes some attacks and also countermeasures. Recently, the security extension KNXnet/IP Secure [7] 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 [5]. A detailed discussion on security considerations for KNX is given in Section 4.

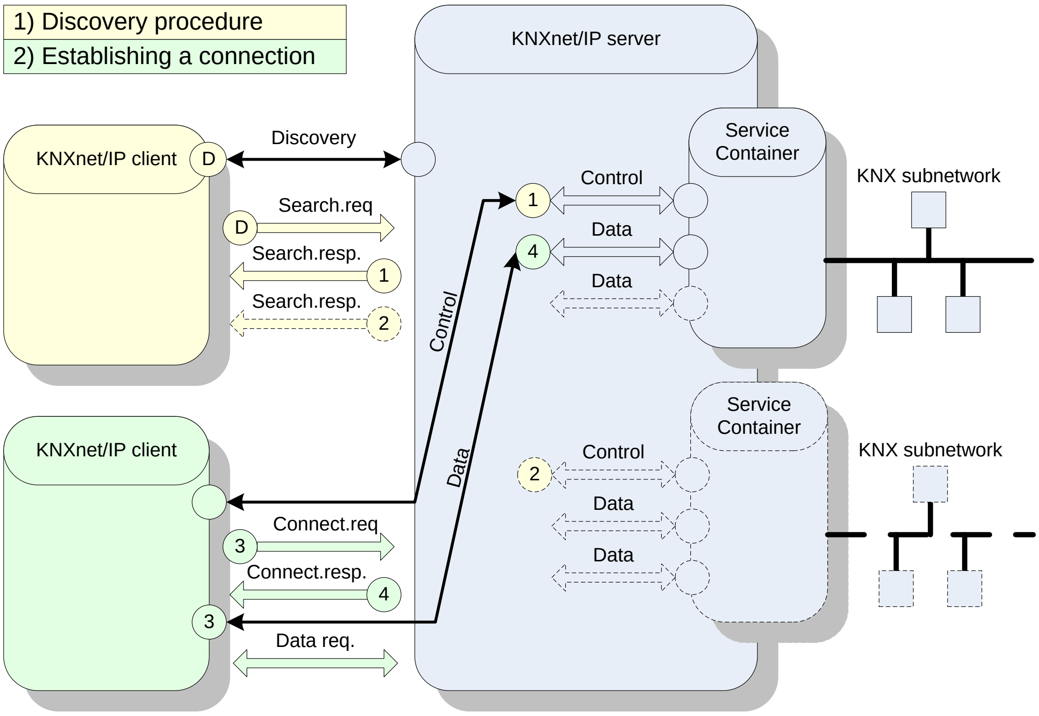


Figure 1: KNXnet/IP discovery

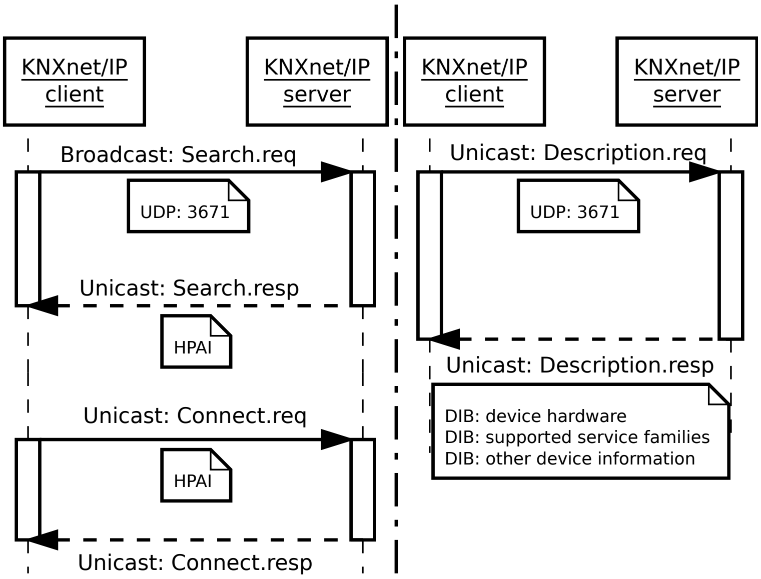


Figure 2: KNXnet/IP communication

3 A survey on world-wide KNX installations

3.1 Attack vector

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

- 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 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 mechanism of KNX relies 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.

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 another device is connected, a non KNXnet/IP standard compliant answer or no answer will be received. If no device is listening to this port at all, no answer will be received.

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 web-cams 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 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 – not only focused on KNX – (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. The average CPU load during scanning 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

3.3.1 Scan 1

Scan 1 started on 6th January 2014 and lasted till 9th May 2014 (cf. [9]). Table 1 shows the *Scan 1* results summed up per country. The installations ranged from business parks and towers, high schools, shopping plazas, water pollution control stations, fire stations, churches to smart homes with control of private saunas (cf. Figure 6). Figure 4 shows the geolocations of the installations in Europe. Figure 5 shows the geolocations of the installations in East Asia. A total of 3.295 KNX installations has been detected. As shown, KNX is very popular in Europe.

For a more detailed analysis, the MAC addresses have been extracted out of the DIBs and their `Organizationally Unique Identifiers` have been used to find out the vendors of the devices. Devices per vendor have been summed up. Figure 3 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.

[9] additionally shows the results of a detailed port scan on all BAS installations found during *Scan 1*. 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.

Country	KNX
DE, Germany	627
NL, Netherlands	522
ES, Spain	332
FR, France	244
AT, Austria	220
CH, Switzerland	204
IT, Italy	173
NO, Norway	129
SE, Sweden	120
BE, Belgium	119
IL, Israel	109
PL, Poland	67
GB, United Kingdom	56
GR, Greece	42
CZ, Czech Republic	30
RU, Russian Federation	24
VN, Vietnam	23
TR, Turkey	21
LT, Lithuania	20
PT, Portugal	20
worldwide	3295

Table 1: *Scan 1* results (top 20 countries)

Country	KNX
NL, Netherlands	427
AT, Austria	142
FR, France	133
ES, Spain	131
DE, Germany	115
CH, Switzerland	92
NO, Norway	87
IT, Italy	83
IL, Israel	73
SE, Sweden	61
BE, Belgium	58
PL, Poland	42
CZ, Czech Republic	27
RU, Russian Federation	19
GB, United Kingdom	19
LT, Lithuania	16
TR, Turkey	15
RO, Romania	14
SK, Slovakia	13
FI, Finland	12
worldwide	1662

Table 2: *Scan 2* results (top 20 countries)

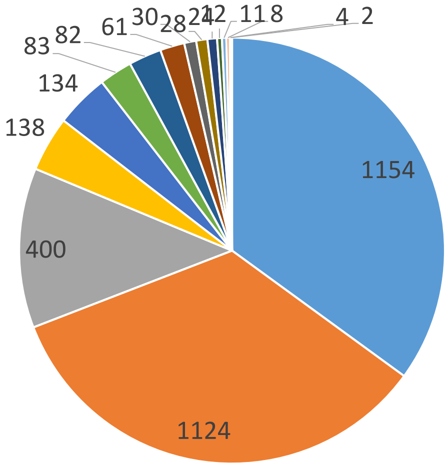


Figure 3: KNX device manufacturers

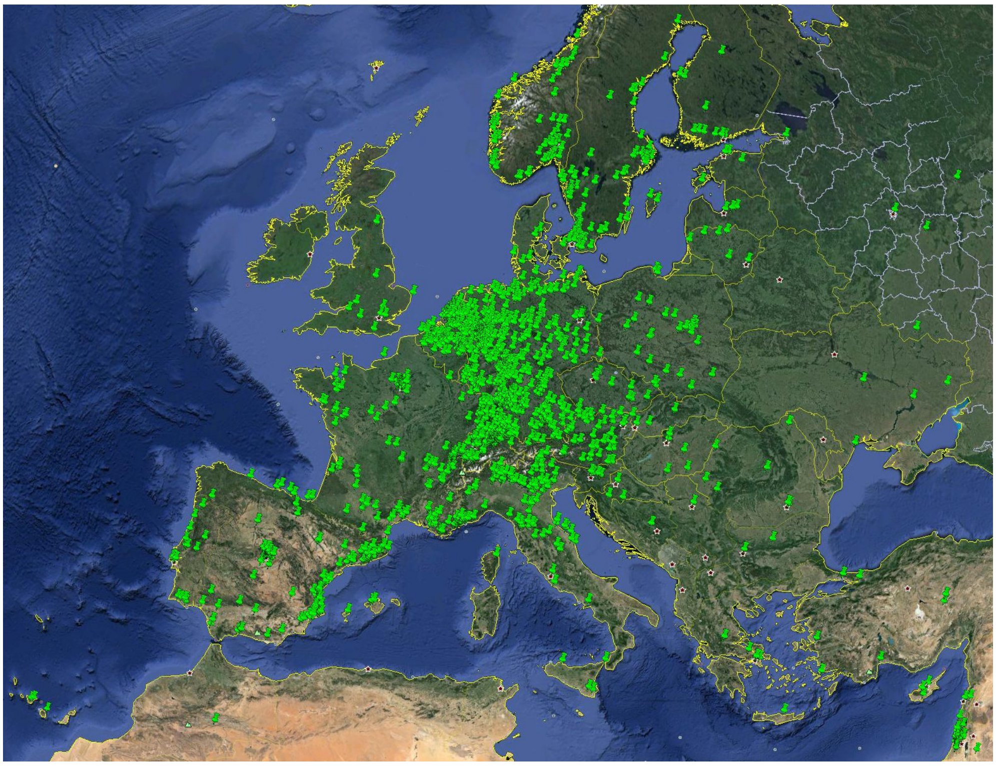


Figure 4: Unsecured KNX installations in Europe

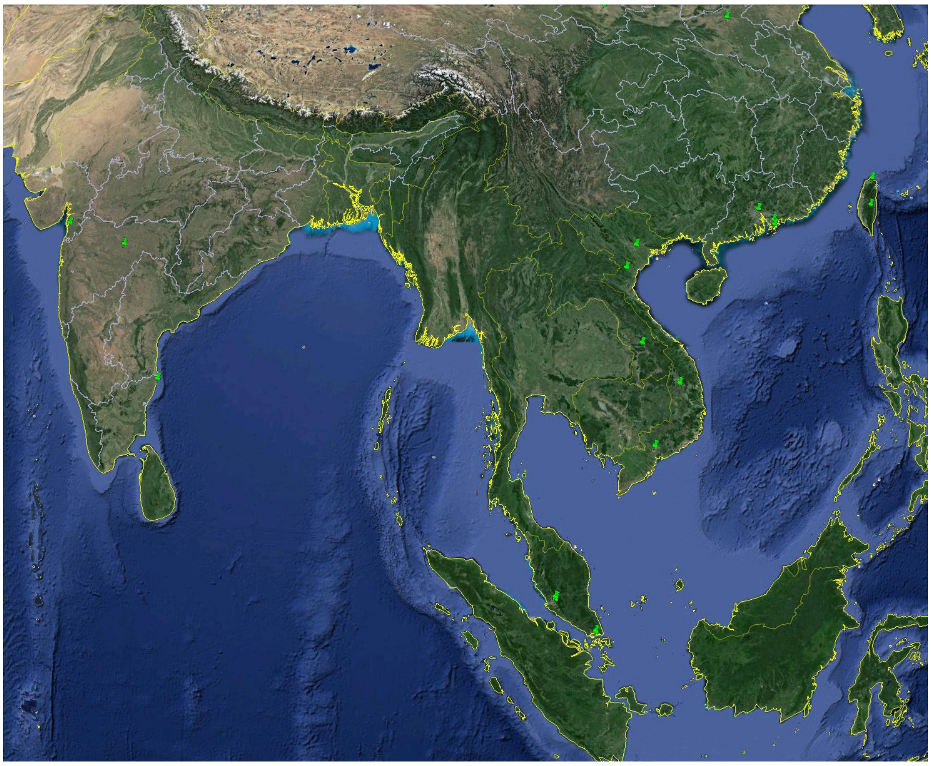
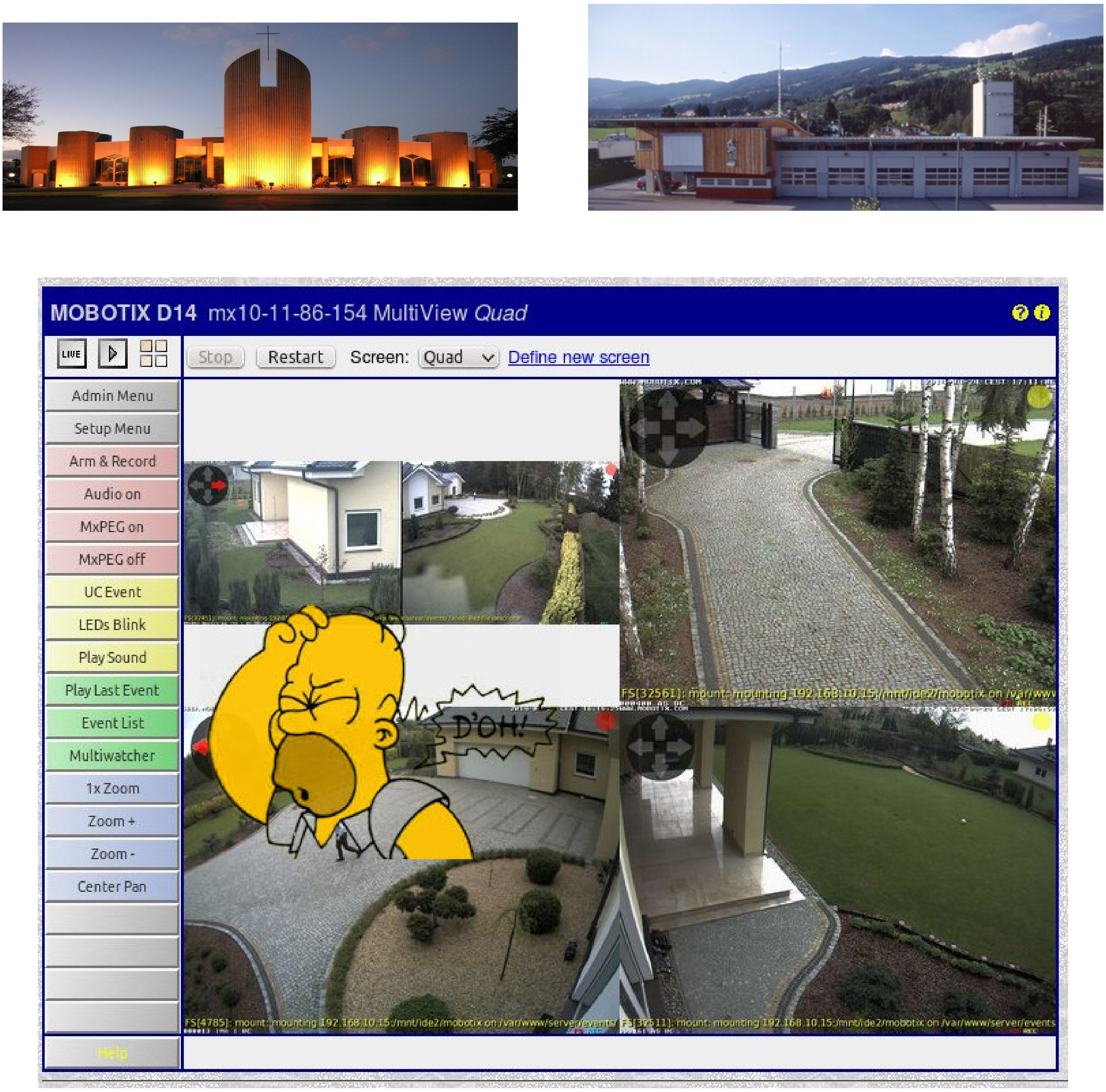


Figure 5: Unsecured KNX installations in East Asia



FS[32561]: mount: mounting 192.168.10.15:/mnt/ide2/mobotix on /var/www

FS[4785]: mount: mounting 192.168.10.15:/mnt/ide2/mobotix on /var/www/server/events/

FS[32511]: mount: mounting 192.168.10.15:/mnt/ide2/mobotix on /var/www/server/events

Figure 6: A more detailed look on KNX installations

3.3.2 Scan 2

A rescan of the previously found installations (*Scan 2*) has been performed on 19th August 2014. Table 2 shows the *Scan 2* results summed up per country. 1.662 out of the 3.295 installations (about 50%) have still been reachable under the same IP. That does not imply, however, that the other 50% of installations can now be considered secure. Most of the (private) installations use a dynamic IP address, obtained from the service provider.

3.3.3 Scan 3

A short third scan (*Scan 3*) with a small subset of IP addresses from countries in Europe lasted from 19th August to 25th August 2014. 375 installations (more than 10%) have been re-detected (identified by their MAC address), which were reachable with a different IP address.

4 Security considerations for KNX

The performed scans during this research show, that security is currently still neglected in KNX installations due to various reasons. First, security features have only been added recently. A lot of current installations (and most of the devices still being sold) use “old” KNX protocols without appropriate security features. Moreover, there is a huge lack of security awareness in the BAS domain. The following subsections briefly discuss the non-functional and functional security requirements and their implementation in the current KNX standard. Comparing, [2] gives an insight into securing distributed and critical infrastructure.

4.1 Non-functional considerations

- Security cannot be gained using security by obscurity (which is especially true for an open standard). A system has to be secure by design. Thus the following statements within the current KNXnet/IP specification [7, 03_08_01 Overview v1.4 p. 11] should be removed:
  - *“(b) Filtering KNXnet/IP datagrams from the network requires network analysis tools and expertise. The content of a KNXnet/IP message is not self-descriptive but requires semantic knowledge residing in ETS. Access to ETS is limited to authorized personnel only.”*
  - *(d) Do not publish default KNXnet/IP IP multicast address.*
  - *It is quite unlikely that legitimate users of a network would have the means to intercept, decipher, and then tamper with the KNXnet/IP without excessive study of the KNX Specifications. Thus the remaining security threat is considered to be very low and does not justify mandating encryption, which would require considerable computing resources.*

  Instead, it has to be emphasized clearly that currently available KNXnet/IP ICDs must not be connected to the Internet. A clear separation between KNX from other services needs to be established (using e.g. Virtual Private Networks). Mechanisms such as firewalls need to be deployed. Security can only be provided using this strict (physical) separation.
- Security needs to be considered for a whole system. Nobody will attack the most secure part of a system, but its weakest point. Therefore, multiple countermeasures and defense in depth need to be deployed.
- Security needs to be seen as a process and not as a one time event. A building’s life cycle typically is 20 to 30 years, it is very likely that security requirements will change during this time. Thus, a secure standard

has to discuss this requirement, which is clearly missing in KNX and other standards. *Scan 1*, also covered BACnet/IP installations. The results are briefly listed here to emphasize this security consideration. BACnet standardized security in 2008 (Addendum g, in standard since 2012 [1]). *Scan 1* revealed, that 13.964 BACnet installations are being connected directly to the Internet. Only in 3 cases security features have been enabled. In all other cases, direct unauthorized access has been possible to the underlying BAS.

- A secure standard needs to cover education (e.g. during certification) covering security requirements and measures. Maintenance, commissioning personnel and integrators are no security experts but domain experts. Simple and clear guidelines have to be available (to e.g. not connect a KNX ICD directly to an office LAN or the Internet). The current KNX Secure webinar covers some general protection measures, but does not explain how to implement them. Typical domain experts (i.e. the ones who finally connect the RJ-45 plug into a KNX ICD) will not be able to implement security using the currently available documentation. Thus, the "usability of security" needs to be improved. A possible central point for such an enhancement lies within the ETS. Integrated security features or a dedicated ETS app could warn the integrator with respect to insecure configurations and could also perform security tests (e.g. detect, whether a KNX installation is directly connected to the Internet).
- During a building's life cycle multiple parties (e.g. electrician, integrator, visualization developer, maintainer) are involved. In fact, it is not easy to tell whom to trust.

4.2 Functional considerations

- Secure communication needs to be provided. [5] shows, that KNXnet/IP Secure provides mechanisms to fulfill this requirement, but further evaluation and testing is required before any security extension can be widely deployed.
- Device attacks need to be prevented to reduce the risk of unauthorized access or sabotage to a KNX installation.
- Secure software architectures (e.g. a secure KNX system software/stack) and an application programming interface need to be provided to be able to develop secure user applications. Update routines need to be available, to be able to address security issues after installation. Embedded systems such as KNX devices need to be likewise update-able as it is common for PCs (e.g. Windows Update).
- Protection to provide availability of installations (e.g. intrusion detection systems) is required.

5 Conclusion and outlook

In order to enhance security in KNX, 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. Immediately, mechanisms such as firewalls helping to prevent access and Virtual Private Networks (VPNs) allowing to connect remote sites need to be deployed.

References

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

[2] J. Akerberg. Towards Securing Distibuted and Critical Infrastructure. In *Proc. 19th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA 2014)*, September 2014.

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

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

[5] 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.

[6] 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.

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

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

[9] F. Praus and W. Kastner. Identifying unsecured building automation installations. In *Proc. 19th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA 2014)*, number 978-1-4799-4845-1, September 2014.

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