ASERCOM cyber-security guideline for connected HVAC/R equipment

Preface

Many HVAC/R components like compressors, fans or controllers have connectivity features today. This includes Bluetooth, Wi-Fi or LAN connectivity. This guideline gives recommendations how to connect HVAC/R components securely to smartphones, other computers or the internet.
The structure of this guideline follows the life-cycle of an HVAC/R installation: it starts with planning and setting up of the architecture, continues with installation of the system, maintenance of the system during lifetime and the guideline ends finally with IT – security recommendations for decommissioning of the installation.
This guideline gives some “hands-on” recommendations for installations in the field with improved security. These steps will help to reduce the vulnerability of installed controllers or inverters but these recommendations are no alternative to an integrated management system. Especially for larger installations / enterprises it is highly recommended to investigate if an information security integrated management system (ISIM) is a necessary step. A good starting point for this investigation can be an introduction into ISO 27001, UL 2900 or IEC 62443:
(see:
https://www.iso.org/isoiec-27001-information-security.html or https://en.wikipedia.org/wiki/ISO/IEC_27001
https://en.wikipedia.org/wiki/Cyber_security_standards
Kobes, P.: Guideline Industrial Security ISO 62443 is easy; Berlin: VDE Verlag; 2017)

It is also recommended to regularly check and follow any local regulations regarding cyber-security which might be in place. Legislation in this field might also change over time.

Image: pixabay

General remarks

Cyber-Security Standards like IEC 62443, VDI/VDE 2182 and others define three different roles in an internet connected installation:

a) The manufacturer of connectable devices like controllers, frequency inverters or sensors (sometimes also called “vendor”)

b) The integrator, who is designing and installing the system in the field using connectable devices (sometimes also called contractor)

c) The asset owner who is using the connected HVAC/R equipment

A very important task for them is communication: information about the specification, the needs, use cases, changes et cetera have to be exchanged between all three of them.

Cyber-Security is not a static goal, achieved once and for all. It is important to maintain this communication and exchange of information (e.g. available updates) during the whole lifecycle of the system in the field. This means, it can be reasonable to establish a PDCA cycle (plan-do-check-act cycle) for the system during the lifecycle.

In the following sections important recommendations are given. Nevertheless, it is important to do an individual risk analysis if additional and more complex measures might be necessary to protect the system. The mentioned steps in this guideline cover mostly technology and processes. Beyond this it is also very important to focus on people: all three above mentioned actors (manufacturer, integrator and asset owner) need to train and sensitize all involved employees to cyber-security regularly.

Not all proposed steps might fit to all installations and applications in the field. It is important to select usable and appropriate steps out of this guideline.

Architecture / Planning

Create a defense in depth design

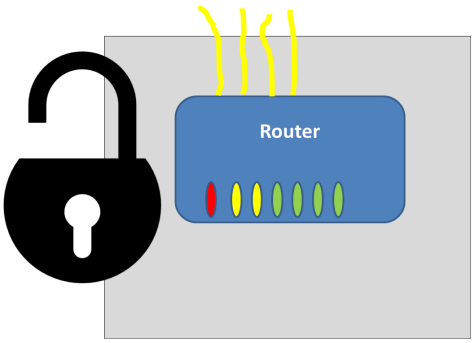
Risk: A single measure to protect an HVAC/R system in the field can easily have weaknesses and can be vulnerable.

Solution: Instead of relying only on a single countermeasure to avoid cyber-attacks it is recommended to use several complementary measures for protection. If an attacker is able to overcome layer 1, the attacker would have to vanquish the second layer and so on.

Place IT components like a router in a locked cabinet / room

Risk: if unauthorized persons have physical access to IT components like a router, firewall, or a PLC, especially with USB-ports etc. they can modify the setup and get access to the installation.

Solution: Place IT infrastructure components like routers or firewall in a locked cabinet or a locked room. Make sure, only authorized people can unlock the door and it is always locked if no authorized people are there.



Separate HVAC/R equipment from other parts of the network (office…) by segmentation (e.g. firewall): segmentation of the network

Risk: If the HVAC/R equipment is in the same segment with office equipment or webservers, cyber-attacks on one part can easily also infect another part.

Solution: Split the installation into logical segments with separated communication (see also https://en.wikipedia.org/wiki/Network_segmentation). This can e.g. be done by implementing a firewall between two segments.

Installation / commissioning phase

Change of default passwords for login (admin and users)

Risk: Components like firewalls or routers but also frequency inverters, controllers or EC fans with a web interface typically have a log-in interface. There is a default login (login name and password) which is described in the manual. If these default logins are not changed an attacker has easy access to the component when the attacker has found out the IP-address of the component.

Solution: The default login (login name and password) needs to be changed during installation.

Delete "installation-accounts" after installation

Risk: Often temporary accounts (admin or user) are set up by contractors during installation. These accounts often have very simple passwords to avoid the need to enter often a long and difficult password during installation.
Solution: Those accounts used during installation need to be deleted after installation is finished or secured with a secure password.

Use passwords containing characters, numbers and special characters with a minimum length of 8 characters

Image: pixabay

Risk: With automated password crackers like *medusa* (part of KALI Linux) it is easy to try thousands of passwords automatically. Those tools typically use password lists which contain passwords found out during previous attacks on internet providers or web applications like ebay.com. They contain frequently used passwords like *123456* or *password*.

Solution: Use more cryptic passwords which are not listed in a dictionary or simply replace an "i" by a "1" or an "s" by a "5". To reduce the risk of a brute-force attack the length of the password should be minimum 8 characters for truly random passwords. Non-random password should be even longer. It is also highly recommended not to use the same password in more than one installation.

Harden the system by closing / deactivating ports, protocols and accessible IP addresses in the connected components

Risk: An IP address of a computer / electronic component can be compared to the address of a house and a port (e.g. 443) or protocol (e.g. https) can be compared to a door into this house. Different web-based applications like email, file transfer or websites have individual protocols and ports. Each open (means accessible) port is a potential cyber risk.

Solution: As HVAC/R equipment typically only accesses a maintenance server and uses only a limited functionality in the web, accessible IP addresses and open ports can be reduced significantly. It is recommended to disable all IP addresses except those few which are really necessary and to close all ports which are not needed. An air conditioning system does not stream videos at youtube.com or needs to communicate with wikipedia.org

Use encrypted data transmission (https, not http; Bluetooth encryption, VPN…)

Risk: If data are transmitted wireless or via a cable without encryption there is always a risk that someone else can eavesdrop this communication and e.g. gets access to login data for an electronic component or system.

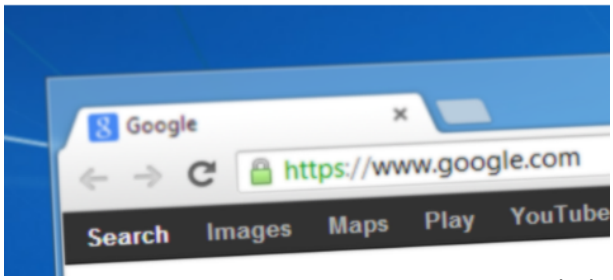


Image: pixabay

Solution: Encryption and authentication on a state-of-the art level should always be used for transmission of data and communication. It is important that the best available technology changes from time to time and it might be necessary to change an encryption method after some time.

Maintenance during the operating lifetime of the system

Install all available updates for firewalls, routers, smartphones/tablets, PCs/Laptops… used in the HVAC/R installation

Risk: Security vulnerabilities are found on a regular basis. Manufacturers and vendors of software and hardware release updates and patches for their products in case the product is affected. If an un-patched component or system is used in an HVAC/R circuit, this system is open for cyber-attacks.

Solution: It is necessary to install all released updates and patches. Many components like firewalls or routers have the option to inform via email or text message if an update is available. Maintenance staff can react in such a case and install the update. Beyond the components and software used on-site at the HVAC/R installation it is also necessary to keep all “tools” like smartphones, laptops or PCs which are temporarily connected to the system updated and patched.

Deactivate Bluetooth / Wi-Fi if not used / needed

Image: pixabay

Risk: There are certain tools and exploits available to attack Bluetooth connections. In free field a Bluetooth connection can be set up at a distance of 50 – 100 m. Other than connectivity via a cable a Bluetooth attack can start from outside the perimeter (closed building or fenced estate).

Solution: In most cases a Bluetooth connection is not necessary 24h / 7 days a week. Often it could be switched off most of the time and only be activated if someone actually wants to transmit data. Hence a significant increase in cyber-security is to deactivate all wireless connectivity when not needed.

Maintain user and admin accounts during the lifetime of the system

Risk: Employees of the asset owner or contractor might leave the company during the lifetime of the HVAC/R system in the field. If the account of such a former employee is not deleted, he/she still can access the internet connected equipment.

Solution: Setup a process to make sure the accounts of all leaving employees are deleted properly. A similar situation happens if the asset owner changes from contractor A to contractor B. If a dynamic password feature is available in the component, it is recommended to use this security feature.

Decommissioning

Reset all components to factory settings and erase all passwords and data. Passwords and data should not be disclosed to anyone after decommissioning in case a password was used in more than only one installation

Risk: If end-of-life is reached for a component or a system it will be decommissioned. In case data are still stored inside the component (e.g. a hard-drive inside a PC or a non-volatile memory (card) inside a controller) those data can be accessed by a third party if the component is disposed.

Solution: Make sure that all data are deleted and all settings are reset to default factory settings before disposing components. Special attention should be paid to memory cards (SD cards) in a card slot, USB flash drives, cloud memory (located in the internet, not on-site) and data on smartphones or laptops.

Revision Index

Revision	Change	Date
A	Initial issue	22.03.2018
B	Final approval	18.07.2018
C	English translation	14.08.2018
D	Print version	22.09.2018

Further *ASERCOM* Statements and Guidelines

- **Hydrocarbon Refrigerants in Refrigerating Systems**
- **Carbon Dioxide (CO2) in Refrigeration and Air-Conditioning Systems (RAC)**
- **Refrigerant Glide and Effect on Performances Declaration**
- **Recommendations for using frequency Inverters with positive displacement Refrigerant Compressors**
- ***ASERCOM* guidelines for the design of multiple compressor racks using frequency inverters**
- **Capacity Rating of Thermostatic Expansion Valves**
- **R22 Phase-Out**
- **Energy Efficiency Rating**
- **Recommended liquid line filter dryers and moisture indicators for refrigeration and air conditioning systems with HFCs refrigerants and POE lubricants**
- **Machinery Directive 2006/42/EC**
- **Pressure Equipment Directive 2014/68/EU**
- **Electromagnetic Compatibility Directive 2014/30/EC**
- **Containment of Refrigerant Compressors**

For more information, please refer to *ASERCOM*`s website www.asercom.org

About *ASERCOM*

ASERCOM, the Association of European Component Manufacturers is the platform for dealing with scientific and technical topics and their challenges, promoting standards for performance rating, methods of testing and product safety, focusing on improved environmental protection, supporting the refrigeration and air conditioning industry and its customers.

Further information is available at: www.asercom.org