Special Issue Published in International Journal of Trend in Research and Development (IJTRD), ISSN: 2394-9333, www.ijtrd.com

Securing IT Networks for Industrial and Building Automation Systems

Nils T Siebel*
Department of Engineering 2, HTW University of Applied Sciences Berlin, Berlin, Germany

Abstract: Automation systems both in industry and building control contexts often require network connections for remote administration and data exchange. This, however, also exposes them to cyber threats like hacking attacks. Hackers may use these machines for a number of purposes like sabotage, sending spam, extorting money by ransomware or to incorporate them into botnets like those used for DDoS attacks. It is therefore important to protect all types of automation and IoT networks from these types of attacks. This article explores the best ways to achieve this necessary protection and gives further recommendations.

Keywords: *IT Security; Cyber Security; Building Automation and Control; Automation*

I. INTRODUCTION

Automation systems control our manufacturing plants as well as the climate and lighting of office buildings, hospitals, schools, universities and factories alike. These automation systems are small computers – sometimes universal controllers like PLCs (programmable logic controllers), sometimes specialised ones like room controllers. These controllers are often connected to the Internet 24/7 to facilitate collection of data as well as remote management. However, they are not always protected against hackers which makes them easy targets. Furthermore, many of them have not been updated with security patches for a long time, resulting in well known security vulnerabilities due to outdated system software.

In this article instructions are given how to protect these networked automation and IoT devices from cyber attacks by designing and modifying configurations of networks and devices accordingly. This entails recommendations for standard automation systems; those used in a critical infrastructure or under especially vicious attack may need considerably more protection effort, the description of which is beyond this article.

II. PROTECTION GOALS

Securing an IT system means protecting it from being tampered with in a way that changes its functionality, uses its hardware and/or exposes or extracts data.

The following basic security aspects are usually considered during the fortification of IT systems against cyber attacks [1, chapter 2]:

1. **Confidentiality** – restricting access to information and systems, e.g. by encryption of data (both during transport and at rest) and by password protection
2. **Integrity** – ensuring that data is not changed (at least not without detection), e.g. when data is transferred online or when we look at a system's web interface
3. **Availability** – guaranteeing access to systems and data when needed; DDoS and ransomware attacks are typical attacks on availability of data and systems, but a power outage (whether it be due to an attack or not) may achieve the same.

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

III. THREATS AND RISKS

Everyone knows that a system that is connected to the Internet is somehow in danger of being hacked. The details of these risks, however, and how this is done are very much less well known, sometimes even among professionals in the automation industry as they are usually no IT professions specialising in cyber security.

Looking at the attacks on many types of automation and IT systems in recent years one can observe the following typical steps of an attack:

1. First, an analysis of the attack surface – the (open) doors into the system – will take place. This includes open network ports exposed to the Internet.
2. The weakest of these openings is used to enter the system or network. If necessary, protections like passwords are overcome at this stage.
3. Once inside the system the attacker tries to gain elevated privileges (gain administrator/root rights) in order to be able to modify operating system (OS) files that are normally protected.
4. With these elevated privileges the OS is changed so that the attack cannot easily be undone, e.g. by changing OS files or installing new executables that run with admin privileges. This may include ways to hide the infection with malware.
5. The system under attack may now be used to attack other systems in the same network.
6. Once the attackers have done their job they can remove the malware and its traces using their admin privileges if they wish to remain undetected.

IV. NETWORK PROTECTION

Traditional IT security has many protections mechanisms and strategies also applicable to networked automation systems.

A. Separate networks

One way to protect IP-based automation devices is by separating their network from the rest of the IT network in a building. This can be achieved by a physical separation (the safest) or a logical separation (more economical).

A logical separation of networks can be achieved by several means. Usually **VLANs** – virtual local area networks – or **VXLANs** – virtual extensible LANs, more flexible – are created for areas of an existing network. These logically

separate areas are still part of a physical network, but the router (or specialised switch) implementing the VLAN inhibits all network traffic between devices which are in different VLANs. Figure 1 illustrates this concept (in this image an "uplink" or connection(s) to other networks are omitted for

clarity). Although all devices could physically communicate with each other through the common router, connections are strictly controlled (here, forbidden).

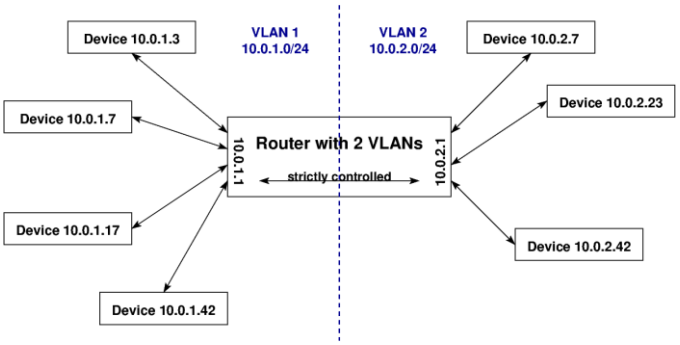

Fig. 1 VLAN – virtual LANs

B. Separation from the Internet

The most effective way to defend from external attacks is, naturally, the severance of the automation network from the Internet. This would again be accomplished by the router, as in Figure 2. Even though the router is itself connected both to the Internet and all IP-based automation devices, it is configured as a firewall to inhibit all incoming and outgoing connections to and from the Internet. It is important to stress that outgoing connections need to be blocked as well, because

- Outgoing connections by automation systems can be used by hackers to exfiltrate (steal) data from a company, for example if connections from other devices are more tightly controlled.
- Many new devices, perhaps most prominently consumer IP cameras, routinely register (via an outgoing connection) on a server set by the manufacturer, thereby facilitating incoming connections through this server, even if all incoming connections are blocked.
- Again many current devices connect to manufacturer websites to upload usage data, possibly violating local data protection laws.

In order to facilitate authorised access from the Internet, e.g. for remote administration or regular data collection from the automation devices, one can use **VPN** – virtual private network – technology to access the network from the Internet, as detailed in Figure 2.

An external computer (e.g. technician's laptop), here with a public IP address of 171.5.21.42, accesses the router through a special public interface. Here a VPN server software is running, which a VPN client software on the external computer connects to. Both the client and the server authenticate against each other, making sure (by the cryptographic methods of certificates) that they are who they claim to be, and that they are directly connected.VPN server and client negotiate an encrypted connection to avoid eavesdropping of data sent across the line. The server process on the router then inserts the external device as a virtual device of the internal automation network, thus allowing it to communicate with the automation devices the same way as a local device.

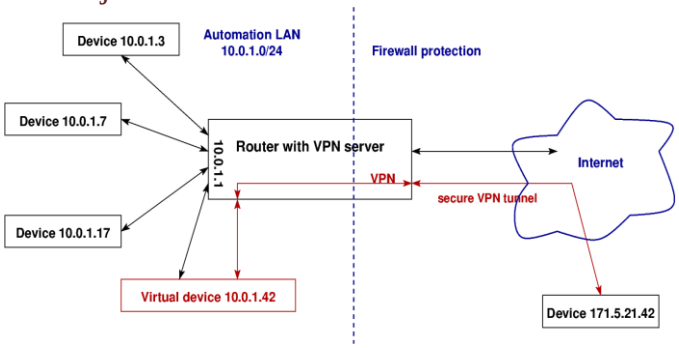

Fig. 2 VPN – virtual private network

C. DMZs

DMZ is another method used in the IT world to separate networked devices from the Internet. Albeit designed for office PCs it can be applied to some automation network setups.

DMZ stands for "demilitarised zone", which is a term originating from military/politics. Figure 3 illustrates what is meant by this in an IT context: a router creates two internal zones: the automation LAN to be protected, and the DMZ. It connects both with the Internet as follows:

- All connections between Automation LAN and Internet are blocked, in both directions
- Both automation devices and Internet devices can connect, in a controlled manner, to devices in the DMZ.
- For any (logical) connection between automation devices and the Internet, a go-between device or service must exist in the DMZ. For example, an automation device can access the WWW with HTTP by contacting an HTTP proxy in the DMZ. The proxy connects to the Web server on the Internet and forwards the web page to the automation device.
- Devices and services in the DMZ must be very well protected (usually hardened GNU/Linux servers); these may also filter traffic, e.g. scan connection traffic for virus signatures, block unwanted content etc.

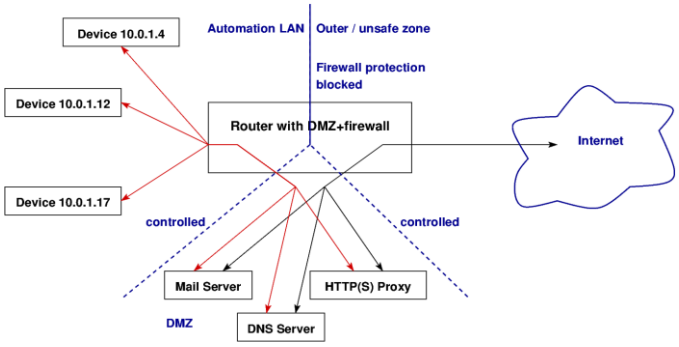

Fig. 3 DMZ – demilitarised (network) zone

D. Individual access control

In order to increase protection, devices within the automation network need to control access. This includes

- Good, individual password per device
- Hindering automatic password guessing by rate limiting login attempts and dynamic blocking upon failure
- Stopping all services and closing all incoming connections ("listen" ports) not needed for operation, like unneeded ftp or telnet access.

- Ideally, limiting all incoming connection attempts access to a small white list of allowed sources.

Connection between devices should also be encrypted and the encrypted connections secured by certificates, if possible.

IV. FURTHER CONSIDERATIONS

Security professionals always stress that the most dangerous attacks **originate from the inside** – a worker or ex-worker might attack their own company. These attackers usually have fewer obstacles to overcome, due to the trust placed in them. Often they have no difficulty attaching a device to an internal network and they may already have access to necessary passwords.

In a related consideration, anyone with **physical access to a device** can usually hack into it very easily – given the necessary skills, of course. This has been demonstrated very impressively by the NSA's supply chain interdiction programme [2]. This is also very much a problem for building automation systems where physical access to devices and networks is usually easier for visitors to the building than for technical staff. A precaution against this – at least for some key devices – is to lock them up in an electrical cabinet and/or in a separate room.

It is not possible to secure a network or device by simply not publishing where it can be accessed. This concept is called "**security by obscurity**" and it is always faulty. For example, there are search engines that you can use look for open administration ports of automation devices – BACnet, Modbus, web interfaces etc. So, having such an open access port and not telling anyone about it does not work – search engines constantly scan all existing IP addresses for these open ports.

Updates to the operating system and running software are difficult with automation devices since they cannot easily be accessed by a technician – most companies avoid remote updates altogether for risk of breaking a system and not being able to repair it quickly. Also, manufacturers often do not publish updates even when security flaws become widely known. Nevertheless, these are essential as serious flaws have existed, e.g. [3] – quickly fixed by updates – and [4] – only fixed after 2 years – both of which enable an attacker to log into a PLC remotely without a password.

It is important to avoid **single points of failure** when securing a network. For example, it is not sufficient to protect access by a password, you also need to restrict access to the password querying interface – the examples given above show that sometimes one obstacle turns out not to be one. It is therefore advisable to have other protection measures in place. This is also called **defense in depth**.

CONCLUSIONS

Securing an automation network – whether it be in a factory or as a building control network – is difficult. However, there are standard methods available from non-automation networks that can be adapted to secure these networks. Sadly, most automation manufacturers, builders and installation contractors have so far been neglecting security aspects but have now been overtaken by reality.

This article was written in the hope that it can help make security methods more accessible and more easily selected in automation contexts.

Terms and abbreviations

BACnet – building automation and control network (standard)
DDoS attack – distributed DoS attack
DMZ – demilitarised zone, a safe (network) area
DoS attack – denial of service attack, targeting availability
HTTP – hypertext transfer protocol, used for web browsing
HTTPS – secure (includes: encrypted) version of HTTP
IP – Internet protocol, used here to mean IPv4 (version 4) only
LAN – local area network (as opposed to WAN)
Modbus – a communications protocol used in automation
OS – operating system
PLC – programmable logic controller
VLAN – virtual LAN
VXLAN – virtual extensible LAN
VPN – virtual private network
WAN – wide area network
WWW – world wide web, the Internet

References

[1] 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.

[2] Glenn Greenwald: "No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State". 1st ed., Hamish Hamilton, London. 2014.

[3] National Cybersecurity and Communications Integration Center (NCCIC) Industrial Control Systems: "Advisory (ICSA-18-044-01): Wago PFC200 Series, Improper Authentication.". Department of Homeland Security, Washington, February 2018, https://ics-cert.us-cert.gov/advisories/ICSA-18-044-01.

[4] National Cybersecurity and Communications Integration Center (NCCIC) Industrial Control Systems: "Saia Burgess Controls PCD Controller Hard-coded Password Vulnerability". Department of Homeland Security, Washington, December 2015, https://ics-cert.us-cert.gov/advisories/ICSA-15-335-01.