TXOne Networks

2022 /Q4

HACKING SMART BUILDINGS:

IoT Attack Surfaces and Defenses

txOne networks

TXOne Networks

HACKING SMART BUILDINGS:

IoT Attack Surfaces and Defenses

txOne networks

Hacking Smart Buildings: IoT Attack Surfaces and Defenses

Table of Contents

The Hackability of Smart Buildings

Imagine your team has assembled for an important meeting. The video conference room beside the data center is humming with the muted sound of air conditioning equipment. Suddenly, security cameras come alive, watching every move you make. Then, the window shades drop, the doors lock, and the heater blasts full-force. The video conference screen wakes up. Ominous red letters glow in the darkness, ***Welcome to the haunted house of hacks…***

You hear colleagues swearing as they try to turn off the video using the touchscreen automation controller. You see cell phones glowing around the conference table. Cell service is dead. Heat warning lights begin to flash on and off. Sweating in the darkness, your mind rewinds past the images of your family. You remember a meeting you had earlier in the week. ***OT Zero Trust. Never trust, always verify.*** You laugh because otherwise, you might cry. The humming from the air conditioners grows fainter as data center systems shut down. You think you smell something strange, then you pass out. Is this a cheesy horror film or a real-world threat?

42% of the world's energy is used in buildings. From special purpose buildings, such as data centers and hospitals, to hotels, office buildings, and even our homes, building automation can improve energy efficiency, safety, and comfort. Whether we're working or living in a building, we expect good air quality, comfortable temperatures, adequate lighting, and safety. Business automation systems can deliver. Those buildings that make use of these systems take in 6% more rent and have a 15% higher sales price. In part, this is because maintenance costs are roughly three quarters of the total cost of ownership. However, these benefits can only be realized if buildings are not "haunted". Since building automation systems connect to the internet and to each other, they are vulnerable to cyber attacks that may haunt you with ransom demands or denial of service. In this situation, think of OT zero trust as the "cybersecurity ghostbusters" of building automation systems.[1]

[1] *Building Facts, Schneider Electric Building Automation & Control Systems, https://www.se.com/us/en/work/products/building-automation-and-control/ (accessed on May 17, 2022).*

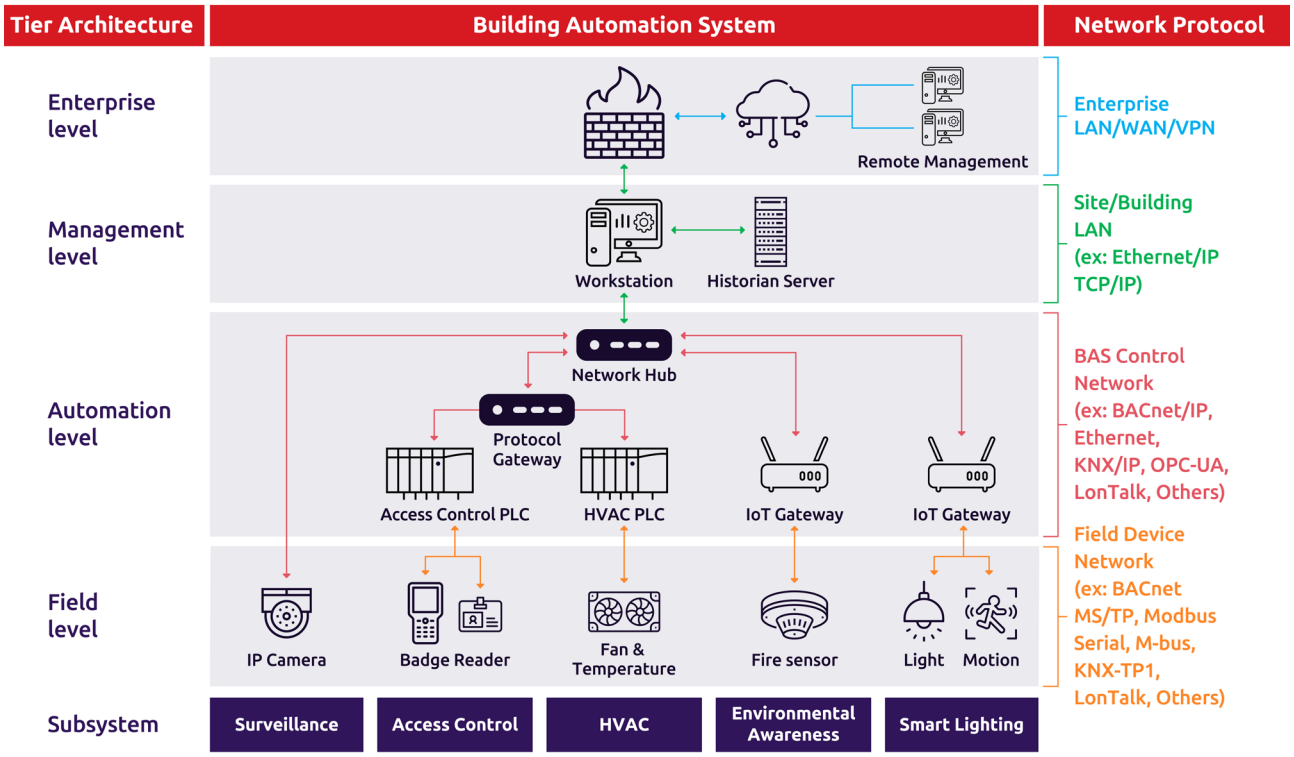


Figure 1 Building Automation System (BAS) Architecture

Building Automation Bedevilments

Assume your building automation system is blissfully undertaking its daily routine, unaware that all the while, an attacker is performing reconnaissance to find openings for an attack. During morning warm-up, the BAS wakes up and checks the weather outdoors. It consults its weather history and decides to turn on the heat so that the building will be cozy by the time people arrive. During the day, the BAS monitors the temperature in zones, so that people on the sunny side of the building are not too hot and people on the shady side are not too cold. Chilled water is often used to cool the air. Cooling towers, pumps, and chiller refrigeration units lower the temperature of the water that circulates through cooling coils in air handling units. Hot water systems heat water and pump it through air-handlers. Heaters are sequenced on and off to maintain hot water supply. Facilities such as hospitals and data centers often require precise temperature and humidity control with no tolerance for variance or downtime. Can the thermometer be manipulated into lying about the temperature, so the heat goes up and up and up? Or, can you turn the heat off altogether and freeze the building?

Lights are turned on or off, or dimmed at any time based on a set schedule or room occupancy. Lighting controllers may detect failures in lamps and ballasts, along with signal failures. Shades ensure that there is no glare, noise, or intense heat or cold coming in through the windows. Dynamic shades such as louvers and shutters open or shut relative to outdoor conditions. Can the lighting schedule, the surveillance cameras, and the shades be tricked into creating total darkness inside a room, the whole floor, or the entire building? How about during surgery?

Laboratories and operating rooms require contaminant-free ventilation. Air handlers optimize energy efficiency while maintaining healthy indoor air quality and proper ventilation. What if the air handlers fail and germs spread?

At closing time, the nighttime setback sets the temperature to conserve energy and turns on the lights in the parking lot. The building automation system stands guard. Security cameras watch for intruders, ready to sound alarms or take action. For example, the access control system can lock doors to create a man-trap around an intruder. In case of emergency, alarms will blare or depending on security thresholds security professionals may receive a silent text alert. Critical alarms repeat. For example, an uninterruptible power supply in bypass mode might repeat an alert every 10 minutes until the problem is resolved. Occupancy sensors trigger burglar alarms when they detect that people are in places at times when they should not be there. Fire alarms and smoke alarms are usually hardwired to override normal building automation schedules so the building can take action to stop a fire from spreading. For example, the BAS might close all the outside air dampers to prevent air coming into the building, and an exhaust system can isolate the blaze. Electrical fault detection systems can turn off entire circuits. Natural gas feed lines can shut down when slow pressure drops are detected (indicating a leak), or when excess methane is detected in the building's air supply. For insurance and liability purposes, a log is being kept of every alarm, indicating who was notified, when, and how.

BAS systems and devices have overrides for manual control. They may also have web interfaces and remote management systems. After discovering where a BAS may lack sufficient defenses, a bad actor sets forth executing the initial attack, aiming to persist by evading detection while bedeviling building automation.

Identifying Security Breaches in Smart Buildings

BAS attacks are similar to ICS attacks, but there are some key differences. Like ICS assets, building automation devices are vulnerable to injection as well as memory corruption, if their code lacks sufficient built-in security. Heirloom building automation systems may still operate legacy versions of protocols such as BACnet with CVE-2019-12480, which has a segmentation fault that could lead to denial of service in BACnet APDU Layer. An unauthenticated remote attacker could cause a denial of service because there is an invalid read in bacdcode.c during parsing of alarm tag numbers. Another situation is one where devices act like zombies, executing every command they receive without question. If bad actors can reach a network with heirloom devices, then they can control them. Imagine your building becoming a botnet of zombie devices (a digital army). In another scenario, attackers can use penetration testing tools like the Nmap scripting engine (NSE) to explore KNXnet/IP protocols, BACnet/IP, or Modbus-TCP protocol vulnerabilities. The Nmap tool helps to identify KNX gateways via unicast discovery messages while in default scan mode. It also provides message bus monitoring functions to read vulnerabilities on the message bus. Originally, this was to facilitate passive information gathering for functions like motion sensors, but now they can be exploited as vulnerabilities that can be attacked by RCE.

Allowing IoT devices inside a building introduces a new threat that is unique to building automation systems. Clever attackers may craft a rogue temperature sensor from a Raspberry Pi computer or find an unsecured UDP port on a device that is still using its default password. In most attacks on ICS systems, the attack begins when a staff member brings a threat onto the work site or the IT-side defenses fail—threats often move laterally through the network until the malware finds a machine where it can inject its payload. Attackers may be able to breach the BAS network without having to craft phishing emails because searching SHODAN or Censys reveals hundreds of thousands of IoT devices with known vulnerabilities. A sophisticated hacker could simply write a script to read the search results, then upload malware into each device on the list.

Another difference is that the physical processes to maintain a building are less complicated than industrial controls. To disrupt production, malware must take into account safety measures, timing, and environmental conditions that are generally stricter than those of a BAS.

1. MITRE ATT&CK PATH for BAS

The path for attacking the BAS could conceivably take four (or even three) steps from the MITRE ATT&CK framework:[2]

1. **Initial Access** – gain access through an IoT device or PLC
2. **Lateral Movement I** – move to a workstation (optional if the PLC is accessed first)
3. **Lateral Movement II** – move to a PLC
4. **Execution** – disrupt the normal functioning of the PLC
5. **Persistence** – infect automation level devices

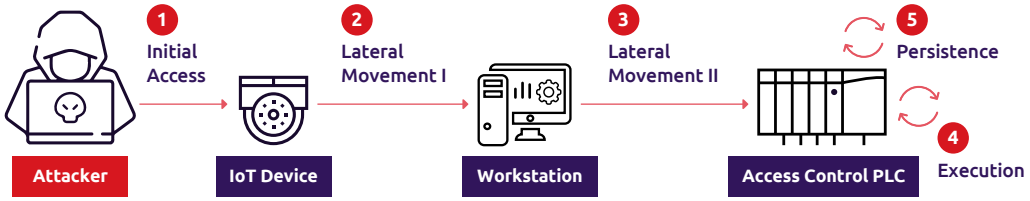


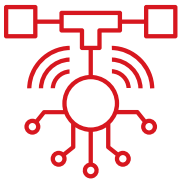
Figure 2 An Example for MITRE ATT&CK PATH of BAS

2. Threat Levels

Currently, the main security threats to BAS are people who intentionally or accidentally reconfigure a device or send possessed control commands instructing a device to take a bad action. The Schneider Electric Secure Development Lifecycle describes four threat levels. Level 1 threats are borne of accident or circumstance, usually resulting from common user mistakes. Level 2 threats are intentional, but relatively simple and often associated with insider attacks. Level 3 focuses on attacks by a trained hacker looking to steal personal, or sensitive, information or corporate secrets. Level 4 attacks come from highly-skilled and well-funded actors working together. These are generally associated with espionage or state actors taking over critical infrastructure such as banks, hospitals and airports.[3]

[2] *ICS Matrix, MITRE ATT&CK, https://attack.mitre.org/matrices/ics/ (accessed May 17, 2022).*
[3] *Get Secure: End-to-End Cybersecurity Lifecycle Frameworks, Schneider Electric Whitepaper (2017), https://www.se.com/us/en/download/document/998-20140821/ (accessed May 17, 2022).*

3. BAS Communication Protocols



Threat actors prey on communication protocols to possess BAS devices. Some devices may communicate over TCP/IP. Others communicate using BACnet, Modbus, LonTalk, or other IP or non-IP protocols. Most devices comply with IEEE 1905.

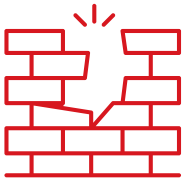
High level controllers may be generic programmable logic controllers, but typically, each building automation company sells a controller for their specific application. High-level controllers interface with lower-level controllers, input/output devices, or a human interface device. They may communicate through open protocols such as BACnet. The American Society of Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE) began developing BACnet late last century. Since then, Siemens, along with other companies, have pitched in to add improvements. In 2003, BACnet was approved as ISO 16484-5. BACnet/IP was troublesome because it provided interoperability but lacked cybersecurity, which made it too risky to open the system to data sharing, alarm and event management, trending, scheduling, and remote device and network management. BACnet/SC eliminated the most problematic elements such as broadcasts, static IP addresses, and the lack of encryption and authentication. It also works well with firewalls, network address translation (NAT), and proxy devices common in IT infrastructure and cloud computing.[4] BACnet apps are available for HVAC control, fire detection and alarm, lighting control, security, smart elevators, and utility company interfaces.[5]

However, despite the building industry's adoption of BACnet Secure Connect (BACnet/SC) to enhance network security in buildings, many legacy systems continue to use outdated communication protocols due to the longevity of OT environments. This leaves these systems vulnerable to interception and tampering by attackers.

[4] *KEY CONSIDERATIONS WHITE PAPER BACnet Secure Connect: The next generation of OT security for building operations, Siemens Whitepaper (2021). https://assets.new.siemens.com/siemens/assets/api/uuid:a450472e-bfbf-4fff-b8a1-b98a22bce1b7/cybersecurity-for-building-operations-white-paper-by-siemens.pdf*

[5] *BACnet – A Tutorial Overview, American Society of Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE) BACnet, http://www.bacnet.org/Tutorial/HMN-Overview/sld023.htm (accessed May 17, 2022).*

4. Breaking and Entering



There are several ways to gain unauthorized access to a building control system: an unsecured IoT device, insider threat, poorly constructed web apps, a poorly configured PLC and so on. Even though there are hundreds of pages of guidance about how to prevent SQL injection and cross-site scripting (XSS), these entry points still exist in web applications used to control (or remote control) building systems. Researchers recently found XSS useful in breaching HVAC and access control PLCs.

Once inside, threat actors can exploit occupancy schedules that control lighting, locks, and temperature. For example, an attacker locked all the rooms in a hotel in Austria and demanded a ransom to open the doors. Residents of a Finnish apartment building suffered in the cold for almost a week when the heating system was similarly hijacked. In hospitals or labs, adjusting locks and temperature can go beyond discomfort and into dangerous spoilage of medicines or chemicals. Unexpected interruptions can damage equipment or facilities and may even cause fires or floods.

5. Freezing in Finland during Heater DoS

A distributed-denial-of-service (DDoS) attack hit the Domain Name System (DNS) of an apartment building in Finland. The BAS that controlled the heating, hot water, and ventilation systems repeatedly rebooted until the system stopped working entirely. Building operation specialists could not connect remotely and had to travel to the site. The problem was resolved by disconnecting the system from the internet. While this incident did not cause permanent, life-altering damage, the lack of awareness about cybersecurity could easily pose a significant threat to the health and welfare of occupants and the building itself, according to Levi Tully, AP PMP, a member of ASHRAE.[6]

6. KNXlock-ed Out of Your Building

Imagine being a building automation engineering firm and suddenly losing contact with hundreds of your devices: light switches, motion detectors, shutter controllers, and more. That's what happened during the KNXlock hack. An attacker gained access through an unsecure UDP port left exposed to

[6] *Mary Kate McGowan, "BUILDING AUTOMATION SYSTEMS: ADDRESSING THE CYBERSECURITY THREAT", ASHRAE Journal, vol. 61, no. 7 (July 2019) reprinted at https://www.ashrae.org/technical-resources/ashrae-journal/featured-articles/building-automation-systems-addressing-the-cybersecurity-threat (accessed May 17, 2022).*

the public internet. They took over the digital security key designed to protect the system and purged the programming, essentially turning hundreds of devices into zombies that they could remote control. Responders had to manually flip on and off the central circuit breakers in order to power on the lights in the building. Then, they removed the hijacked BCU (bus coupling unit) password from memory. Fortunately, the attacker used the same password for all the zombies, so they were able to restore the BAS programming more quickly. The responders could have used brute force to decipher this password because it is only a 4-byte string with eight characters. However, the device reboot time was slow, so they opted to pluck it directly from CPU memory.

This attack has been dubbed KNXLock because it targeted KNX-based systems. It was interesting because bad actors turned a security feature into an attack vector. KNX added a warning on their website that if the user's password is lost, the device should be returned to the manufacturer because the BCU key cannot be changed or reset externally. This would render the password protection meaningless.[7]

7. Credentials Theft

Tridium systems allow remote management of devices from an IP camera with open-source video recording software to HVAC PLC or badge readers with proprietary control software. A vulnerability was found in one version of the Tridium Niagara AX Framework that allows an attacker to remotely access configuration data including usernames and passwords. As shown in Figure 3 admin with encrypted password. A hard coded secret key was discovered in one version of the software that allowed this password to be decrypted.

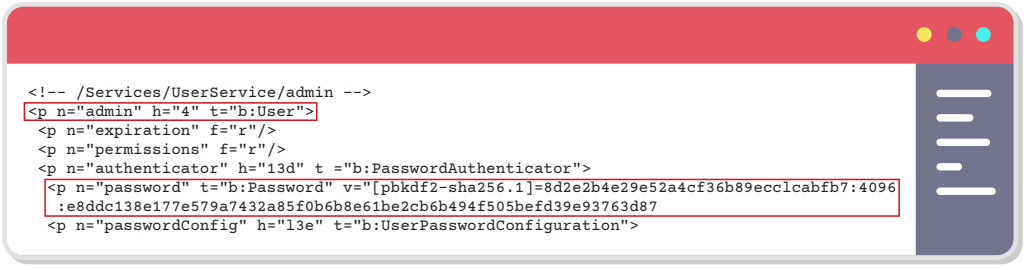


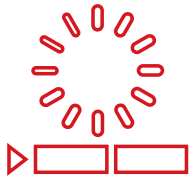
Figure 3. Sample config.bog file showing username: admin with encrypted password.[8]

By deciphering these credentials, an attacker can login and issue control commands. Other attacks allow privilege escalation, granting the attacker further access. While these may not be zero-day attacks, using the SHODAN search engine reveals that many systems are visible over the internet.

[7] *Kelly Jackson Higgins, "Lights Out: Cyberattacks Shut Down Building Automation Systems", Dark Reading (2021). https://www.darkreading.com/attacks-breaches/lights-out-cyberattacks-shut-down-building-automation-systems (accessed May 17, 2022).*

[8] *Google's Buildings Hackable, https://blogs.blackberry.com/en/2013/05/Google-s-Buildings-Hackable (accessed May 17, 2022).*

8. Buffer Overflow



A daemon runs on an access control PLC that exposes multiple HTTP endpoints for remote management. One of the HTTP endpoints can be used to see if the system is up. However, if you send it a long sequence of characters in the HTTP request, then it crashes. Researchers verified the long sequence causes a buffer overflow.

9. TCP/IP Supply Chain Vulnerabilities: Ripple20

Ripple20 refers to 19 vulnerabilities found in the software developed by Treck, Inc. for processing TCP/IP network traffic. The vulnerabilities are in the low level stack and masquerade as legitimate traffic. Four of these enable remote code execution. One vulnerability is in the DNS protocol. Other vulnerabilities open the door for denial of service (DDoS) attacks.

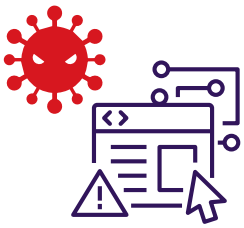
Ripple20 reached IoT devices from a wide range of vendors because Treck collaborated with ELMIC before the two companies went their separate ways, both unknowingly selling the infected software. Now, in addition to Treck and ELMIC, this infected software is also known by other names: Net+ OS, Quadnet, GHNET v2, and Kwiknet.

Ripple20 poses a significant risk from infected devices that are still deployed. Potential risk scenarios include an attacker from outside the network taking control over an internet-facing device inside the network. A bad actor who has already infiltrated a network can use the TCP/IP library vulnerabilities to target specific devices or to broadcast an attack capable of taking over all infected devices simultaneously. An attacker may use an affected device to stay hidden in the network until they are ready to launch a full-scale assault. A sophisticated hacker could craft a MITM attack or DNS cache poisoning to hack a device inside the network and bypass NAT configurations. In all scenarios, a threat actor can gain complete control over the targeted device remotely, with no user interaction required, much like a ghost taking possession of a person.

Four Cornerstones for Building Systems

Granted, being locked in your own conference room, and held hostage for ransom seems more like a reboot of ***Panic Room*** than a typical workday. But is it so far-fetched? The sole function of building automation systems is to create a comfortable indoor environment. Without safety controls, a hacker could become a poltergeist haunting your house, hotel, hospital, data center, sports arena, or even cloud-based services client businesses rely on. OT zero trust offers four cornerstones for cybersecurity: inspect, lock down, segment, and reinforce. The overarching idea is to never trust, always verify.

1. Inspect



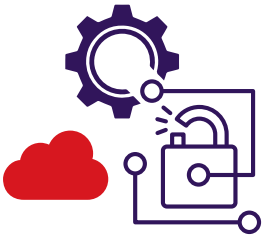
Inspect every device that is part of the building automation system. The most common way scary software enters an organization's BAS is by trusted people either intentionally or inadvertently bringing it in. Organizations also need a process to identify and manage security risks for all externally sourced components. This can be done using automated tools to monitor and track vulnerabilities. Using a handheld security scanner, an organization can find and destroy malware before the device is deployed. Inspections stop many supply chain and insider attacks.

2. Lock Down

Use allow lists and trust lists to lock down endpoints and network traffic. These lists function like virtual security guards posted at every virtual entry way into your BAS. They adapt to the current circumstance and assess the trustworthiness of each situation. They may be a straightforward list used by fixed-use assets or a trust library of common OT, BAS, or ICS applications and certificates. Trust listing promotes fast operation and resource availability for necessary building operations. Take this a step further with one more layer of endpoint protection, which comes in the form of machine learning that can spot suspicious activity without interrupting trust listed processes.

At the network level, control commands and other messages flow through security zones on a "need-to-know" basis. Everything else is blocked. Disallowing specific commands requires an OT-native appliance that can understand BAS protocols such as BACnet and prevent hackers from sending malicious commands, both by strictly limiting privileges and by setting suspicious or unusual commands to be blocked by default. This approach works best with network segmentation, where these privileges can be defined to cater to the specialized needs of each asset. It's critically important for BAS defense to shelter each endpoint's specialized needs, covering heirloom systems for legacy jobs as well as modern assets that handle a variety of tasks.

3. Segment



Segment your network into zones that are more easily defended. However, to further enhance network segmentation and provide in depth defense, it is advisable to adopt the concept of "Zones" and "Conduits" as outlined in the IEC62443 standard. A "security zone" refers to a group of physical or logical assets with shared security requirements and defined boundaries. The connections between these zones, known as "conduits", should be equipped with security measures to control access, prevent denial of service attacks, shield vulnerable systems in the network, and maintain the integrity and confidentiality of communication. Use OT native protocol policies to specify approved commands and IP-based policies to determine which assets can communicate with each other. The fundamental tools of network segmentation are the OT IPS and OT firewall appliances. A next-generation OT IPS can divide critical assets into micro segments or groups of assets that require 1-to-1 protection. Next-generation firewalls transparently create segmentation and use a broader definition of network security policies. Work site-friendly "OT-native" IPSes and firewalls can be deployed transparently without changes to existing BAS architecture. Trust lists can be set at both the network level and at the protocol level. Network segmentation informed by OT zero trust allows for isolating or aggregating vulnerable assets into a safe zone that is more easily kept away from zero-day attacks and other dangerous cyber threats. In some cases, assets play such an important role in building systems that they can never be taken offline. Network segmentation with OT zero trust-based policies prevents attackers from traveling within your network to reach these high-risk machines.

4. Reinforce

Reinforcing cybersecurity depends on a lot of factors. Is a security patch available? If it's available, is it compatible? Does the OT environment allow for the asset to be patched? Asset status and patch status are constant considerations within the maintenance process. Using virtual patches, assets are protected without making changes to their configurations, regardless of whether or not their manufacturer has released a security update. Technicians use virtual patches to reduce risk until it's the right time for an update and a vendor-supplied patch has been released and tested. They can also reinforce protections indefinitely for otherwise unpatchable heirloom assets. The OT-native IPSes and firewalls that make this kind of asset-centric cyber defense possible have rule sets specifically designed to repel attacks without forcing endpoints to conduct an update. There are no system reboots and no production downtime. Engineers can keep assets operational and secure while they prepare the patch for deployment during a scheduled maintenance window.

Conclusion

While there is no silver bullet for cybersecurity, by securing building automation systems with the OT zero trust approach, buildings are more comfortable, energy efficient, and safe. The first step in increasing security is a secure supply chain: organizations should require partners throughout the supply chain to meet a reasonable level of security. They should integrate their security requirements into their terms and conditions and evaluate vendors for potential protection gaps. They also need a process to identify and manage security risks for all externally sourced components. This can be done using automated tools to monitor and track threats and vulnerabilities.

Second, OT zero trust architecture: in the future, we will see more and more IoT devices applied to smart buildings. Organizations can trust four cornerstones: inspect, lock, segment, and harden. Think of OT Zero Trust as the "cybersecurity ghostbusters" of building automation systems. This saves building engineers a lot of development time and expensive safety engineering expertise.

Third, the total lifetime protection of OT endpoints: OT endpoints in smart building fields have to be used for over 20 years, but for the cybersecurity team, managing legacy endpoints and systems will become the new norm. If there is no long-term asset protection or visibility, serious security problems will arise. An asset-centric approach is needed to support endpoint lifetime protection, thereby safeguarding endpoint applications, monitoring legitimate processes, and preventing malicious programs from running amok.

Appendix

Smart Elevators

Connectivity takes elevators and escalators to new heights of availability and efficiency. VIPs can call the elevator concierge to gain immediate access. Elevators send real-time data to maintenance personnel, as well as download software updates on demand. During a fire or an evacuation, elevators and escalators respond to these emergencies with voice notifications and in-car video displays. Firefighters can take over elevators to help them arrive where they are needed to fight the fire.

Connectivity also opens the door to cyber threats. Software updates leave the system vulnerable to supply chain malware unless the source and integrity of these updates is verified. Cryptographic tools are useful in beefing up security, but they require extra computer horsepower. According to the magazine Facilities Management UK, an attack is unlikely to be able to cause an elevator car to crash because elevators rely on mechanical safety brakes. Most modern-day elevator car crashes occur during maintenance or in old, obsolete elevators. However, a bad actor could use the elevator remote management system or the firefighter overrides to gain access to other BAS systems or to compromise the availability of elevators. These cyber threats are being taken seriously by elevator manufacturers around the world.[9]

In 2019, the National Elevator Industry Inc (NEII) in collaboration with the European Lift Association (ELA), the Pacific Asia Lift and Escalator Association (PALEA), and China Elevator Association (CEA) published the ***Elevator and Escalator Industry Cybersecurity Best Practices*** guide. It follows the ISO 14798:2009 risk-based approach as supplemented by the NIST Cybersecurity Framework, IEC 62443, and others.[10]

In-Home Systems

Historically, commercial and industrial buildings relied on protocols such as BACnet while home systems used proprietary protocols. In 2013, IEEE 1905.1 was adopted with a common interface for home networking technologies. A couple years earlier, the QIVICON alliance had been formed by companies from different industries to collaborate on cross-vendor, wireless home automation solutions for smart homes. Since then, they have been working

[9] *Nigel Stanley, "The Cybersecurity Risks of an Elevator Ride", Facilities Management UK (fmuk:202), 12. https://content.yudu.com/libraryHtml/A43wv7/FMUKApril2020/reader.html?page=12&origin=reader (accessed May 17, 2022).*

[10] *Elevator and Escalator Industry Cybersecurity Best Practices, National Elevator Industry, Inc (NEII:2020) https://nationalelevatorindustry.org/wp-content/uploads/2020/08/NEII-Cybersecurity-Best-Practices-7_16_20-1.pdf (accessed May 17, 2022).*

towards the goal of safely connecting controllable devices made by different manufacturers. Motion detectors, smoke detectors, water detectors, wireless adapters for power outlets, door and window contact sensors, temperature and humidity sensors, carbon monoxide sensors, thermostats, cameras, household appliances, weather stations, sound systems, and lighting controls can exchange data.[11] Now the difference between commercial and home systems is largely just the size of the system.

Digital Twins and Other Trends

According to ***Verdantix 10 Predictions For Smart Building Technology in 2021 and Beyond***, digital twins may be used to improve the efficiency and safety of the BAS through a continual feedback loop between real sensors and their virtual copies, aka digital twins. Schneider Electric and Bentley Systems rolled out digital twins at Microsoft's Frasers Tower in Singapore. Employee engagement apps will become more popular as people return to the office. Data from the BAS will inform a central mobile communication hub so employees can interact with elevator buttonas, room comfort controls, audio/visual devices, digital badges, building safety systems, and building navigation using these apps. Edge computing devices will move data processing closer to data sources in order to realize improved response times, reduced bandwidth load, lower energy consumption, and increased data security.[12]

CVEs[13]

CVE ID	CVSSv3	Description	Potential Impact
CVE-2020-11896	10	Triggered by sending multiple malformed IPv4 packets to a device supporting IPv4 tunneling. Affects any device running Treck with a specific configuration. Can allow a stable remote code execution and has been demonstrated on a Digi International device. Variants can be triggered to cause a Denial of Service or a persistent Denial of Service, requiring a hard reset.	Remote Code Execution
CVE-2020-11897	10	Triggered by sending multiple malformed IPv6 packets to a device. Affects any device running an older version of Treck with IPv6 support. Previously fixed as a routine code change. Can potentially allow a stable remote code execution.	Out-of-Bounds Write
CVE-2020-11901	9	Triggered by answering a single DNS request made from the infected device. Affects any device running Treck with DNS support. Can perform Remote Code Execution on a Schneider Electric APC UPS. Severe because DNS requests may leave the network and a sophisticated attacker may be able to take over a device from outside the network through DNS cache poisoning or other methods to infiltrate the network. The malformed packet is almost completely RFC compliant and difficult to detect by firewalls, etc. On very old versions of the Treck stack, the transaction ID is not randomized, making this attack easier.	Remote Code Execution

[11] *QIVICON, https://en.wikipedia.org/wiki/QIVICON (accessed May 17, 2022).*
[12] *Dayann Charles Jeyamohan and Susan Clarke, "10 predictions for smart building technology in 2021 and beyond", Verdantix (Verdantix:2020) https://research.verdantix.com/report/10-predictions-for-smart-building-technology-in-2021-and-beyond (accessed May 17, 2022).*
[13] *19 Zero-Day Vulnerabilities Amplified by the Supply Chain, https://www.jsof-tech.com/disclosures/ripple20/ (accessed May 17, 2022).*

txOne networks

txone.com