CYBER DEFENSE MAGAZINE

eMAGAZINE

MARCH 2023

In This Edition

Zero Trust in a DevOps World

Eight Tips for CISOs Trying Get Their Board on Board

Solving Cybersecurity Problems Arising in "Difficult Environments of High Uncertainty."

...and much more...

MORE INSIDE!

Zero Trust Cybersecurity Safeguards New Devices in Smart Buildings

When hardening corporate networks, zero-trust architecture and product patching can mitigate cybersecurity concerns

By August Johnson, Sr. Product Cybersecurity Architect - Global Product Security, Johnson Controls

New classes of embedded devices are joining today's corporate networks to help optimize building operations, reduce resource use and improve occupant well-being. At first glance, these new embedded devices seem like conventional hosts, much like employee workstations. They need IP addresses, certain levels of outbound connectivity, and software updates.

However, the security controls and policies in most buildings have not evolved at the same pace as these smart technologies. Trying to fit these devices into processes designed for conventional hosts like corporate laptops can result in insecure configurations and an increased network risk for cyberthreats.

System hardening with the right lines of defense can minimize the threat when new devices are added to the network and make these hosts even easier to securely manage than standard corporate laptops and servers. Establishing a high level of device security includes consistent, planned patches and strong authentication.

Maintaining a patching cadence

For years, PC operating system and web browser providers have been offering reliable, automated monthly updates for their consumer products as a security best practice. In comparison, many smart devices are designed with hardware constraints and long production cycles that can prevent devices from maintaining sufficient security protection. It is common for an embedded device like a network-connected room controller to be built with a processor that was designed a decade ago or more. Devices can sit on shelves for months or even years before deployment, and security patches can become outdated as time passes.

Purpose-built hardware devices usually require manual effort for each firmware update. These updates are released on a vendor's schedule, which can occur infrequently (annually or even longer) with some releases skipped entirely. Without established processes built around a reliable patching cadence, these devices may not be equipped to protect against the latest cybersecurity risks. Manufacturers that do not support regular, timely updates for their products have not established a solid foundation for cybersecurity.

Devices with outdated patches may not be protected against all current cyberthreats, and the consequences of these threats can differ based on the purpose of each embedded device, even when devices are in the same network and have the same basic hardware. Device usage can range from ordinary, like a connected HVAC system used to improve occupant comfort in an office building, to life-threatening, like hospital operating room air quality controls. Understanding the difference between use cases is important to hardening a network and managing devices.

Considering device life cycles and applications

Device replacement time is also a potential drawback of embedded devices. Replacing a corporate laptop can happen within hours, but a failed embedded valve controller or connected chiller will likely require a special order to procure and a specialist to replace for optimal operational continuity.

In addition, the lifespan of a corporate laptop is predictable, while the lifespan of embedded devices can vary wildly, from nearly disposable to multidecade replacement cycles. Requiring a mature patching program for a connected chiller likely to see two decades of service is important. Software updates for a disposable food shipping safety sensor with a short service life may not be as critical.

Understanding the device's application is also important when determining patching needs. If an outage or cyber event results in a bank's marquee thermometer displaying the wrong temperature, there's probably little consequence. However, if a freezer used to store vaccines uses the same network-connected thermometer hardware to determine safe storage, compromise can easily result in an expensive loss. Patching is therefore more necessary in the vaccine application.

Establishing the security of embedded devices

An organization that is purchasing and deploying embedded devices must commit to a process for identifying and applying updates. If products are not hardened and data is lost or compromised, organizations can experience a range of consequences. These include disruption of operations and negative publicity that can result in lost revenue and reputation damage.

Without strategic planning, the security level of a device can become outdated over time. In some scenarios, a vendor may have no incentive to offer patching after a device is sold or may go out of business and be unable to provide critical security patches. Strong commitments from vendors that include regular, timely updates can help resolve these risks and can be obtained before a device is purchased.

Since embedded devices are hosts on the network, they will have some sort of network traffic. This traffic requires monitoring just like the other hosts on the network. If there is a back door on these devices, it is important to ensure a consistent traffic monitoring process is in place to identify the device if operational anomalies are detected.

The constrained nature of device hardware also means that there are limits to how much data can be accessed at the device level, if at all. Many buildings use a central hub to aggregate and clearly display data from all the devices on a network and control commands sent to embedded processors. This hub usually has a web interface that allows users to visualize trends and track key parameters as well as control each of the connected embedded systems. A compromised hub may be used to push implicitly trusted but malicious updates to the devices on its network. This is why hardening the hub system itself is critical to hardening the network.

Since these hosts are centralized and often have many integrations, applying the principle of least privilege, a security tactic that allows users or entities only the access required for a specific task, can close many points of entry for cyberthreats. Unauthorized and expired user access needs to be managed to reduce the threat of compromised accounts. Achieving a high level of network security takes expertise and continuous effort, and leading vendors offer hub solutions that streamline network management in the form of software-as-a-service. Centralization by the vendor can shift software patching incentives in the right direction.

Zero Trust Architecture

Obtaining the trusted identity of each individual device is a foundational step for connected building network security. Cryptography can help with this, whether it is manufacturer-embedded keys, or a cleanroom process for initial device identity provisioning. A strong, securely granted, centrally-managed identity at startup is a required step in a secure deployment.

As these hosts are connected to the corporate network, rules defining network-level access should be written. This is where embedded device hardware constraints start to become an asset. The access mapping is usually small and simple, and unlikely to change, in contrast with an individual's laptop.

Building an accurate map of access needs is not only possible, but a very important task in the deployment checklist.

With strong device provenance and a well-managed hub, the wires that connect them become points of weakness. The challenge now becomes ensuring data in-transit is secured. The details of managing this are device and vendor specific, but transport-layer encryption remains a very strong control against unwanted intrusion in corporate networks.

The bases for zero trust architecture includes strong encryption for device identity and data-in-transit, as well as a whitelist-only access control list. Zero trust architecture minimizes risk by limiting breach opportunities, containing the damage of any actual breach and surfacing unusual behaviors quickly. Embedded devices fit well into these deployment paradigms because of their relatively static mission, and low complexity roles on the network.

In a hypothetical attack against an embedded surveillance system, a remote attack may be avoided with consistent, planned patches and strong authentication. Sometimes attackers use a widget to patch into the physical line between a camera and the hub, but since zero trust protected devices use both encryption and authentication in-transit, this connection is protected against compromise.

Finally, an attacker may try to physically replace the camera with their own compromised camera on a loop, but without a trusted cryptographic identity, it will be rejected. By only allowing connections between continuously authenticated and authorized entities, zero trust security can establish advanced self-defense systems and smarter buildings that are more resilient to cyberattack.

About the Author

August Johnson is a Product Security Architect for OpenBlue Solutions at Johnson Controls. In this role, he works with development teams to deliver connected experiences to power healthy buildings. Solutions range from simple embedded systems to machine-learning enabled analytics. As an architect, August has been helping software teams build security into their products in the insurance and healthcare industries in the past. To learn more about Johnson Controls holistic approach to cybersecurity visit our cyber solutions website at https://www.johnsoncontrols.com/cyber-solutions.