This article was published in ASHRAE Journal, July 2021. Copyright 2021 ASHRAE. Posted at www.ashrae.org. This article may not be copied and/or distributed electronically or in paper form without permission of ASHRAE. For more information about ASHRAE Journal, visit www.ashrae.org.


David J. Branson

Understanding IIoT Cybersecurity Issues

BY DAVID J. BRANSON, P.E., BCXP, FELLOW/LIFE MEMBER ASHRAE

Applying cybersecurity principles to the built environment often focuses on securing user access to building automation systems, an obvious area of concern. Similar application can secure the interface that connects equipment to the internet to facilitate machine-to-machine communication—often referred to as the Industrial Internet of Things (IIoT).[1] A cursory knowledge of this subject is important to give owners, engineers and technicians a user-level understanding of cybersecurity issues. After all, the development efforts mentioned in this column are being funded directly or indirectly by all of us. In a way, this means we are also funding cyber criminals.[2]

A primary function of the IIoT is to allow field devices to pass collected low-level data through edge node and relay devices to cloud services that can provide advanced processing in support of complex decisions, and then possibly allow the return of instructions for equipment use. Examples include diagnostics and operational adjustments to prevent early hardware failure, real-time utility purchasing, resource optimization, strategic planning and other advanced features.

Many methods exist to allow developers to move data between devices in the IIoT world, and more are being added rapidly. Organizations like OASIS[3] (see the "Terminology" sidebar for acronyms and definitions) have released tools and methodologies to aid in the development of secure communications between devices along independent paths. OSI[4] network, transport and framework functional levels are typical focal points of cybersecurity intrusion, and they form the domain of this introductory column. The goal is to allow manufacturers, developers, specifiers and users of equipment in the built environment to better understand the ease with which these appliances can be secured.

Most of us have been exposed to the networking OSI model. Internet protocol (IP) resides at the OSI network layer; HTTP[5] and TCP[6] reside at the transport layer. Additional transport layer protocols are widely available for use by developers of IIoT services. Common examples are MQTT,[7] CoAP[8] and DDSI-RTPS.[9] These foundational tools allow data to pass between disparate appliances.

Equipment manufacturer developers use these and other protocols to pass data between computational tools that reside on dissimilar compute platform configurations, e.g., an x86-class desktop computer running Microsoft Windows 10 communicating with a cloud application residing on a Raspberry Pi running Debian Linux operating system (OS), with service tech input via a smartphone running its unique OS. Without this cross-platform capability, shared or advanced cloud services would be severely limited by hardware compatibility.

IIoT cyberattacks usually occur at the communications interface of a device in the pathway used to transport

David J. Branson, P.E., is president of Compliance Services Group, Inc., in Lubbock, Texas. He is a member of TC 1.5, Computer Applications and vice chair of the Cybersecurity Multidisciplinary Task Group.

data. With that in mind, appliances being used can be scrutinized to determine which cyber-hardening tools could be used. Some of these tools, like the encapsulation of data to be used at end node equipment via encryption/decryption algorithms, can greatly increase the robustness of data security and significantly reduce the chances of a successful cyberattack. Encapsulation can in certain instances be expensive, both in funds and time, and many other potential solutions exist; they are beyond the scope of this column. An evaluation of required rigor and resources should be made to determine acceptable choices of appliances to use in combination or outright for a good cybersecurity solution.

Some cyberattacks come by way of hardware disruption to gain access to the target system. Firewalls are available as software apps that run on systems that host the data or as appliances that stand between the internet and the protected equipment. Firewall devices can be very simple but effective, or complex and feature rich. The extent of equipment being protected and overall throughput requirements will dictate where a firewall will sit along the cost line. Properly sized uninterruptible power sources and order of start-up and shutdown sequences are critical for proper use of firewalls.

Studies have revealed an amazingly high number of equipment exposures to cyberattack due to use of default or poorly constructed login/password combinations. This should not be the problem it currently is, as it signals a casual approach to system security. Someone that recognizes the importance of security should be tasked with keeping systems secured. Employees should be trained how to maintain login/password sequences.

Dated equipment often lacks sufficient hardware, software or firmware flexibility to support security protocol updates. This is a common exposure point for attack. Where equipment updates or upgrades are cost-prohibitive, stand-alone appliances can be considered for insertion at communication connection points to provide dedicated protection.

Terminology

Industrial Internet of Things (IIoT), an evolution of a distributed control system (DCS) that allows for a higher degree of automation by using cloud computing to refine and optimize the process controls.

Organization for the Advancement of Structured Information Standards (OASIS), a global nonprofit consortium that works on the development, convergence and adoption of open standards for cybersecurity, blockchain, Internet of Things (IoT), emergency management, cloud computing, legal data exchange, energy, content technologies and other areas.

Open Systems Interconnection (OSI) Model, a widely used conceptual framework that describes the functions of a networking system.

Hypertext Transfer Protocol (HTTP), an application layer protocol for distributed, collaborative, hypermedia information systems.

Transmission Control Protocol (TCP), a common protocol that provides reliable, ordered and error-checked delivery of a stream of octets (bytes) between applications running on computing hosts communicating via an IP network.

Message Queuing Telemetry Transport (MQTT), a lightweight publish-subscribe protocol to transport messages between devices.

Constrained Application Protocol (CoAP), a specialized protocol for use on constrained network devices, e.g., low-power, lossy networks.

Data Distribution Service Interoperability–Real-time Publish-Subscribe Wire (DDSI-RTPS), a protocol for machine-to-machine data exchange using a publish-subscribe pattern.

References

1. Ranger, S. 2019. "What is the IIoT? Everything You Need to Know About the Industrial Internet of Things" ZDNet.com. https://tinyurl.com/4p5bar7k
2. Trend Micro. 2021. "Cybercriminals." Trend Micro. https://tinyurl.com/26hhztpa
3. OASIS. 2021. "OASIS Open." Organization for the Advancement of Structured Information Standards (OASIS) https://www.oasis-open.org/
4. Geeks for Geeks. 2020. "Layers of OSI Model." GeeksforGeeks.org. https://tinyurl.com/ybvj4jds
5. MDN Web Docs. 2021. "An Overview of HTTP." MDN Web Docs. https://tinyurl.com/pt6zxnax
6. Lutkevich, B. 2020. "TCP (Transmission Control Protocol)." TechTarget Network. https://tinyurl.com/86833n7x
7. MQTT. 2020. "MQTT: The Standard for IoT Messaging." MQTT.org. https://mqtt.org
8. CoAP. 2016. "RFC 7252 Constrained Application Protocol." CoAP.Technology. https://coap.technology/
9. Object Management Group. 2019. "DDS Interoperability Wire Protocol." Object Management Group. https://tinyurl.com/kwufmad7 ■