The Evolution of Operational Technologies

Is IoT a Threat?

Bryan Marklin- Consultant

As the Operational Technologies (OT) ecosystem evolves, one of the constants is the adoption of "Open" networking capabilities. These OT systems include Access Control, Video Surveillance & HVAC among others. Whether wired, WiFi, cellular or one of the low bandwidth methods, these network capabilities present new opportunities for those with malicious intent. This document is intended to be a brief on the network technologies and possible risks being introduced to building owners & operators.

IoT in general has become a ubiquitous term- Nest thermostats & Ring doorbells are among the most recognizable to consumers. Think of IoT as anything, typically a device that is network capable. IoT security breaches have become well documented in healthcare and perhaps the best known, Target's data center which was attacked through a back door in their HVAC network. The victims of public hacking penetration suffer not only monetary loss, additional costs can be their reputation, the faith of their investors and perhaps worse yet, their customers trust.

Many OT platforms have a very small attack surface. Systems that are hard-wired, analog and not connected to a public network have a very small attack surface. When the manufacturers "enhance" their products to support open network standards and network connectivity, the attack surface grows exponentially. What makes OT systems so vulnerable is WHAT these systems control and how MANY networks they can be connected to.

Manufacturers view IoT as a great way to gather data about their systems. How they are performing, are they in need of maintenance, etc. Johnson Controls "Smart Connected Chillers" is a great use case to look at. JCI states in their own literature:

"Here's how they work: Johnson Controls collects data from the chillers, stores it on our platform in the cloud and accesses it via an application used by our internal service technicians. With this app, they can evaluate the condition of the chillers and receive alerts to identify and solve potential problems with the units. We've recently launched a customer-facing portal so that they also can analyze data to better understand how their chillers are performing."

https://www.johnsoncontrols.com/buildings/specialty-pages/connected-chillers

Seems like a good thing, right? Gathering information to help you better help your customers should be harmless. For clarity, this isn't a "JCI thing", it's an industry thing. Most manufacturers were focused on gathering data and did not give a thought about Cybersecurity concerns. Even JCI says they gathered and analyzed the data and then later, offered their customers the ability to view their own data.

The risk is how the manufacturers SEND (and/or receive) the data. I will share some first-hand experience as a proof point. A large hospital chain in Ohio was testing an IoT security device to protect medical devices. After the second week of their Beta test, the VP of Network services informed me that they were under a cyber-attack. “Shut down your systems!” which is what my field engineers did immediately. The probing attack (hackers typically “probe” the network to discover topology, etc.) continued and the VP had every available resource begin to shut down all non-essential systems. Ransomware attacks were on the rise and most were devastating, hackers would encrypt electronic medical records or other crucial systems. The hospital would have to pay a ransom within a certain timeframe to get the encryption key to restore their records.

12 hours and countless IT resources were expended only to discover that one of their vendors had serviced their chillers and installed new flow and temperature sensors. These IoT sensors were probing the network and trying to get to the internet to “phone home”. This hospital had state of the art tools and trained staff yet, you can’t protect what you are unaware of. Good intentions do not necessarily equate to a secure outcome.

“Even though a majority of the organizations are beefing up security on the IT side, they are leaving the doors to their OT “wide open,” which allows “basic threats such as ransomware and malware to step right in and catch them.” (CSOonline.com)

https://www.csoonline.com/article/3284481/iot-security-a-concern-but-most-companies-dont-have-a-way-to-detect-attacks-on-ics.html

The key point here is to understand the networks and methods of how IoT, especially OT IoT, connects to the various manufacturers’ cloud and/or analytics systems. This will give you a measure of how large the potential attack surface may be. Let’s take a look at the ways IoT is connecting to the Internet.

Ethernet

Ethernet is the standard for wired networking. Most OT & other OT systems have moved away from proprietary “hard wiring” and standardized on Ethernet. It’s easy and robust and comes with an added benefit over the other connection methods; POE. Power over Ethernet provides the ability to power and communicate with an end-point device. Video Surveillance Cameras and VoIP phones are a perfect use case as it eliminates the need to run separate power to the device. POE has 4 basic classes that provide a few watts all the way up to 100 watts of power. Besides cameras & phones, POE (POE+) can power video conferencing systems, televisions and yes, building control systems. Securing Ethernet networks requires knowledge of security best practices as well as an understanding of how it will be used and where the traffic needs to go.

WiFi

Wireless Ethernet has become commonplace in businesses, campuses and public areas. For many, it’s the go-to solution for IoT connectivity. WiFi has also become very “noisy” (lots of radio channel conflicts) which can negatively impact it’s reach and penetration capabilities. Security can also be a concern because not all Access Points (APs) are not created equal and sophisticated spoofing or monitoring systems. Some vendors are starting to design their APs to also support BlueTooth Low Energy (BLE). More on this later…

Cellular

Cellular Networks literally blanket the country with exceptions in sparsely populated or desolate areas. Many IoT vendors use this to literally take their traffic direct to the cloud, bypassing their customers' network altogether. Some customers may take exception to this as a privacy concern but that is an argument for another day. One of the challenges of cellular is the high cost of components (in the IoT gear) and the cost of the network. With the evolving capabilities of 5G LTE, cellular operators are working to address this. LTE- CAT M (for Machine) is designed to provide much power bandwidth at a much lower price point. Other cellular innovations beginning to see light are IoT CAT-0, IoT CAT-1 and the newest, Narrow Band IoT (NB-IoT) uses the "guard band" between LTE frequencies. NB-IoT is provided by most major cellular providers.

BlueTooth

BlueTooth has developed into a ubiquitous technology that connects devices to devices. Most people are familiar with BlueTooth with the connection of their mobile phone to their wireless headsets. BlueTooth has evolved into a connection method for IoT devices. BlueTooth is rated at 100M but is usually connected to devices within a few meters of each other. BlueTooth Low Energy, (BLE) uses less power than earlier versions while BlueTooth 5.0 greatly increases range so BLE 5 can connect to more IoT devices like lighting, automation and some industrial applications. It's important to note that BlueTooth does not directly connect to the internet, it requires a gateway to do so. As mentioned earlier, some AP (WiFi access points) are natively supporting BLE. BLE support is also being supported in cellular IoT applications.

IoT Devices and Their Operating Systems

Understanding how many networks that IoT devices can connect to is important when trying to evaluate the overall risk. The networks themselves are not the risk, they are the "connectivity path" between your devices and most everything including the Cloud, Analytics and of course, potential hackers. Once you understand all of the "paths" to your devices, you can then put in place the capability to secure or at least monitor that path.

The real risk is the Operating Systems (OS) of the IoT devices, in this case, we will examine one of the major OS brands, VxWorks. VxWorks is a Real-Time Operating System developed by Wind River and released in 1987. VxWorks provides manufacturers with an "Off-the-shelf" OS solution so they can easily build and deploy their various products. VxWorks last release of VxWorks (7) was in 2014. During the 2019 Black Hat Briefing conference, security researchers shared methods created to explore vulnerabilities of VxWorks. A few months later, Armis, a Cyber Security Company released its "Urgent/11" warning on VxWorks and presented their findings at the Black Hat briefing in August,

2019. The Urgent/11 report identifies 11 “Day Zero” vulnerabilities of VxWorks and estimates that approximately 2 Billion IoT devices are at risk. Armis went on to state;

“The URGENT/11 vulnerabilities are estimated to impact devices such as SCADA, elevator and industrial controllers, patient monitors and MRI machines, as well as firewalls, routers, modems, VOIP phones and printers.”

Armis posted a few videos on YouTube to show how easy & quick the vulnerabilities could be exploited. See them here;

https://youtu.be/GPYVLbq83xQ (Sonic Wall Firewall)

https://youtu.be/zdVuSnCq4ac (Patient Monitor)

https://youtu.be/u1DybHV34L8 (Xerox Printer)

The good news is that Wind River has been very responsive and has created security patches to address the vulnerabilities.

The key to this exploit is to take over or shut down devices. When you watched the Patient Monitor video above, what were your thoughts? What if your IoT devices were compromised? HVAC? Elevators? Security systems?

These patches will only help address the Urgent/11 vulnerabilities IF they are installed!

Summary

New IoT devices are growing exponentially. Gartner estimated over 20 Billion IoT devices by 2020. To understand the risk they present to your business, you must understand how others view them, the methods used to connect them and HOW you can best insulate yourself from the risk they can present. Your vendors may have great intentions of how IoT can be used to help your systems efficiency, provide great analytics and alert you to potential maintenance issues. Conversely, if that same IoT system is breached and your business is compromised, records stolen or held as ransom, all those benefits will be negated. It’s wise to understand WHAT your vendors are doing to help you (and themselves) to all that data. For example, is the data (from your facility) going to the cloud encrypted? What security precautions have they taken? Which Cloud vendor is hosting this? Are your systems running VxWorks or other “at risk” operating systems? The more you understand makes you better prepared to evaluate the risks.

When looking at how these IoT devices connect, your organization may be able to exert more control. Many times, OT systems are connected via cheap, off the shelf network components. Your investment is primarily in the systems, not their networks. That alone could provide some security challenges. Not all network devices and especially, the design of that network are created equally. It’s critical to understand that the more networks that are connected to the internet, the larger the attack surface is for hackers with malicious intent.

Technology Plus is an expert in Operational Technology and Security systems. We can help you & your business understand the IoT “Blind Spot”. Contact us for insight into how we can do an assessment and help secure your critical system assets.