www.pipelinepub.com
Volume 18, Issue 1

Mission-critical Cybersecurity for Industrial-grade Wireless Networks

By: Ishaq Mian

Thousands of enterprises worldwide rely on reliable broadband wireless networks for their IoT, voice, data, and video communications needs. It is an essential part of building out and extending network coverage to all users and applications. Due to the shared nature of any technology based on radio frequencies (RF), however, wireless systems can be more vulnerable to security issues than wireline deployments.

High-availability, high-capacity wireless systems require additional levels of security, as these systems are regularly deployed to enable mission-critical and business-critical applications. Methods popular for many private Wi-Fi networks, such as restricting physical access to private areas, reducing RF emission, and site surveys, have become ineffective. A more comprehensive, risk-informed, system lifecycle management-based security approach must be adopted from the beginning, during system planning and design phases.

Mission-critical businesses need a holistic, comprehensive approach to security that will protect wireless data. These systems must also look at the management plane against security threats—such as passive and active attacks—and against physical tampering. In this context, security needs to be discussed as part of the definition of industrial-grade wireless networks.

Cyber-physical systems

In the last several years, enterprises have witnessed a dramatic rise in the development of smart and "context-aware" mission-critical systems that marry embedded computing devices to their respective physical environments.

© Pipeline Publishing, L.L.C. All Rights Reserved.

Not for reproduction or distribution. © Pipeline Publishing, L.L.C. All Rights Reserved.

Systems that use information from the physical environment—and in turn can affect the physical environment during their operation—are called cyber–physical systems (CPSs). The tight integration between the cyber and the physical in CPSs, though advantageous on one level, is subject to new forms of risks. These include the cyber element adversely affecting the physical environment.

In the world of industrial automation, the interdependencies introduced due to the integration of the physical with the cyber and the associated security implications for critical infrastructure are a critical, complex topic of ongoing research.

Deep dive

In June 2010, cybersecurity researchers discovered the first physically destructive cyber weapon targeted at an industrial process. This complex and sophisticated malware, named Stuxnet, forever revealed the vulnerabilities of modern control systems to the industrial world. Although cyberattacks on industrial control systems in critical industries had been happening since the late 1990s, their impact remained limited because of a lack of automation in these industries. The impact of Stuxnet, however, was significant, as it demonstrated that cyber vulnerabilities could lead to degradation of critical physical processes with major implications.

Stuxnet specifically targeted the Siemens SIMATIC S7 Programmable Logic Controllers (PLCs) and WinCC Supervisory Control and Data Acquisition (SCADA) systems responsible for controlling and monitoring the high-speed centrifuges essential to the uranium enrichment process at a government facility in Natanz, Iran. The malware successfully modified the rotational speed of the centrifuges, leading to major random system faults.

Since then, the cybersecurity of CPSs has gained critical importance in industrial environments. In fact, it has evolved into a separate branch of general cybersecurity in which the systems being protected have physical characteristics which, if compromised, can lead to downtime, injury or death, and economic loss. Regulatory and standards bodies have developed and employed a security function in which security features of industrial-grade wireless networks are prioritized for OT before anything else. What this boils down to is that industrial-grade wireless networks must manage the risks inherent in integrating the cyber with the physical.

Compliance is essential in an industrial environment. Industrial-grade wireless networks follow strict security standards and guidelines, specific to critical industries, and protect against CVEs, or common vulnerabilities and exposures. Most cyberattacks in industrial environments have involved unpatched systems, legacy equipment, and vulnerabilities in underlying networks.

Initiatives such as NVD18 (National Vulnerability Database) and CVE19 provide vulnerability databases with standardized identifiers to facilitate communication of information about common vulnerabilities in software products to industry professionals and the public.

Modern wireless networks leverage operating systems and software products. This can expose an otherwise-secure industrial control environment to cyber vulnerabilities. Given this reality,

© Pipeline Publishing, L.L.C. All Rights Reserved.

Not for reproduction or distribution. © Pipeline Publishing, L.L.C. All Rights Reserved.

industrial-grade wireless networks must leverage operating systems that remain up to date on patches and issue fixes for CVEs as a continuous process.

A physical attack on a network device that makes the network unavailable or injects a malware inside the network can lead to data leakage, or even remote control of an ICS component. For example, in 2017, an employee used a USB drive to download and view a movie on a critical infrastructure computer in the Middle East. The user did not realize that this action released malware—later dubbed Copperfield—by Nyotron, the company responsible for detecting it. Copperfield resulted in data leakage, network scanning and remote control of an ICS workstation.

Similar physical-to-cyberattacks can happen when an attacker gains physical access to a networking device with weak local authentication and launches a cyberattack by making the network unavailable. Industrial-grade wireless networking devices implement hardware security controls to prevent physical tampering.

It is also important to remember that OT systems differ from traditional information technology (IT) systems in their cybersecurity priorities. IT systems manage information, whereas OT systems manage physical processes.

The primary function of OT is to enable safe working environments and protect capital-intensive assets while maximizing overall system uptime availability. The goal of ensuring the integrity of stored data and protecting the data's confidentiality is important to OT systems, but usually secondary to the goal of availability.

In the world of IT, on the other hand, data confidentiality is primary, followed by data integrity—and then maintaining a high degree of availability. It is this difference of priorities that often leads to heated debates among IT and OT professionals within critical industries when discussing optimization of resource allocation to secure a network. The United States National Institute of Standards & Technology also highlights this difference in its guide on industrial wireless systems deployment.

Generally, IT systems defend against data extractions; encryption used to provide confidentiality is of primary concern. In OT systems, confidentiality is still important but secondary to availability. While eavesdropping can provide access to information, which can facilitate a future cyberattack or reverse engineering of proprietary methods and design, confidentiality cannot be achieved at the expense of system downtime. Overall, to secure the physical environment, industrial wireless networks need to focus on these key pillars:

Authentication

Authentication is a method used to validate that a device or user is authorized to gain network access and that the source of data is genuine. Authentication is an important aspect of industrial security linked to process availability—and can be more important than the concept of encryption. Devices within a network must be authenticated and industrial-grade wireless networks should support device authentication.

© Pipeline Publishing, L.L.C. All Rights Reserved.

Not for reproduction or distribution. © Pipeline Publishing, L.L.C. All Rights Reserved.

Encryption

Encryption, or the method used to encode data to prevent unauthorized access to the data, is important to both wired networks and wireless networks. It is important to verify that the level of encryption that a candidate wireless network uses will meet the needs of the security risk level of the industrial ecosystem. Throughout, these networks need to follow cryptographic protocols such as Diffie-Hellman.

Ease of implementation

Industrial-graded wireless networks make securing wireless deployments easy to implement and maintain.

Default security and updates

Network devices must be set to the highest security level by default to protect against man-in-the-middle attacks and spoofing. Also, industrial-grade wireless networks must provide the capability to disable automatic updates along with the ability to update firmware over the air or wire.

Share and report

Vendors of industrial-grade wireless networks perform analytics, continually learn about security, and share security threat data with regulators and the larger community.

Full lifecycle

Industrial-grade wireless security must cover the entire lifecycle, from product development through deployment, operation, and retirement.

Passwords and spectrum monitoring

Industrial-grade wireless networks support the implementation of password change policies. In addition, these networks need to use spectrum monitoring efficiently to gain awareness of normal versus abnormal wireless activity.

Mission-critical Cybersecurity: In Summary

It is important for IT professionals to recognize that wireless security practices used in the office may not be available for industrial deployments. The most important message to all users and developers of industrial-grade networks is that security is part and parcel of the definition of mission-critical, and technologies must assure that both cybersecurity controls and cyberattacks do not limit or prevent the capability of the system running with the highest availability factors.

© Pipeline Publishing, L.L.C. All Rights Reserved.

Not for reproduction or distribution. © Pipeline Publishing, L.L.C. All Rights Reserved.