HIRSCHMANN

A BELDEN BRAND

White Paper

WP00008HE

A Construction Kit for Secure Wireless Network Design

Tobias Heer
Head of Embedded Development – Functions Hirschmann Automation and Control GmbH

Bernhard Wiegel
Lead Engineer – Wireless Hirschmann Automation and Control GmbH

Table of Contents

Executive Summary

Security has always been an important consideration when applying wireless technology in industrial applications. Influenced by discussions in the IT world, the perceived threats often relate to a loss of confidential data or intrusion by an attacker. As a result, industrial control system (ICS) security discussions are often reduced to the need for encryption mechanisms.

Modern security procedures, however, offer much more than data encryption. Topics, such as central access control systems, intrusion detection, firewalling and the protection of management frames, are also important components of a comprehensive security concept.

Another critical aspect of ICS security is deploying multiple layers of protection to guard critical assets. Through an approach to security called Defense in Depth[1], both overt and unintentional external and internal threats can be detected, isolated and controlled. While this white paper will describe several defense solutions, reliance on one solution can expose a system to a single point of failure. Defense in Depth is a far more effective strategy for reliable ICS security measures as it incorporates several complementary and overlapping technologies.

While evaluating security needs, it is often difficult to see the big picture in the maze of various technologies and strategies. This white paper classifies the different security mechanisms available for wireless network design and describes their effects and limitations using examples from a variety of industrial applications.

Be certain.
Belden.

While most wireless office networks can cope with short downtimes and disruptions, mission-critical machines cannot tolerate such problems without interrupting their operation, and ultimately impacting the bottom line.

Identifying the Security Needs of Industrial Wireless Networks

Communication with wireless local area networks (WLANs) opens up a wide variety of new possibilities for industrial applications. At the same time, poorly configured wireless communication systems introduce new risks to the network and the industrial applications that rely on it.

In the consumer and enterprise environment, the term security is often equated with confidentiality because theft of information is the primary threat. Within industrial applications, reliability, availability, integrity and authenticity generally are the most important requirements, with confidentiality being a slightly less important consideration.

While most wireless office networks can cope with short downtimes and disruptions, mission-critical machines cannot tolerate such problems without interrupting their operation, and ultimately impacting the bottom line. This is why attack scenarios in the industrial sector not only target data and password theft, but also focus on the disruption of control and monitoring mechanisms in the production process. IT administrators would opt to shut down the network to prevent confidential information from leaking – choosing confidentially over reliability – but if the same philosophy was applied by OT managers, an improper shutdown of the network could destroy the process – the exact thing security measures try to protect against.

One shocking example of such an attack is the destruction of a steel furnace as reported by the German Federal Office of Information Security (BSI) in 2014.[2] In this case, a process communication disruption caused the destruction of the production equipment due to an improper shutdown of the plant.

It is important to keep these different requirements in mind when considering potential attacks and countermeasures for industrial applications. We must consider what actions are required to protect an industrial wireless network.

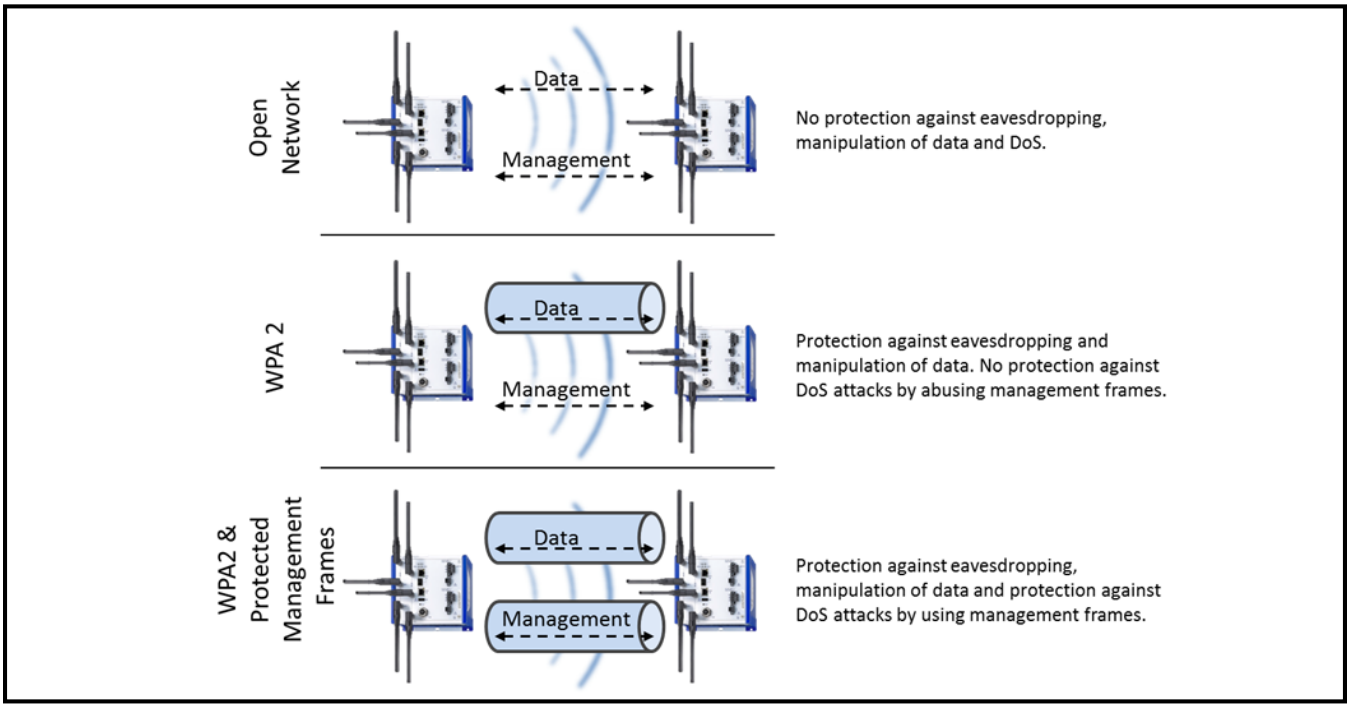

Figure 1: Open networks offer no protection at all. A network that is secured with WPA2 prevents wiretapping and manipulation of data. Networks that provide Management Frame Protection based on IEEE 802.11w also protect the management messages that are important for availability.

Assessing ICS Security From the Outside In

To frame the discussion, this white paper considers the route of an attacker from the border of the network (e.g., an attacker without WLAN passwords) to the core of the network (e.g., an attacker who is already present in the WLAN). On this route through an industrial network model, we examine and discuss the possible threats and countermeasures that are possible.

We also incorporate examples throughout this white paper of how to follow a Defense in Depth strategy when considering these threats and routes. For our purposes, Defense in Depth is built on three core concepts:

1. **Multiple layers of defense:** Layering multiple security solutions so that if one is bypassed, another layer will provide the defense. Systems cannot rely completely on a single point of security, no matter how good it is.
2. **Differentiated layers of defense:** Sound security strategy, whether military, physical or cyber security, makes sure that each of the security layers is slightly different. If an attacker finds a way past the first layer, they don't automatically have the capabilities for getting past all the subsequent defenses.
3. **Threat-specific layers of defense:** Each of the defenses should be designed to be context and threat specific. In essence, you should design for the threat. For example, a system can be exposed to a variety of different security threats, ranging from computer malware and angry employees, to Denial of Service (DoS) attacks and information theft. Each needs to be considered and defended against. This allows defenses based on the behavior and context of the systems using these protocols.

Consideration should be given to each of the threat areas by layering the technologies and strategies discussed in the next sections to protect your system.

Protecting the Edge of the Wireless Network

Unlike solutions for wired data transmission, wireless LAN radio communications are difficult to limit and contain within an area. Therefore, a WLAN can exceed the company's property boundaries and attackers do not necessarily need direct physical access to an industrial network in order to interfere with it. Since we cannot prevent access to the physical transmission and reception – Layers 1 and 2 of the International Organization for Standardization's Open Systems Interconnection (OSI) model[3] – it is essential that we find other ways to secure them and ensure reliable operation of the network and connected plants.

Without appropriate security in place, the signals of a WLAN could be received and understood by an attacker, and as a result, confidential information and data from the network could be captured. Attackers could also feed incorrect information or control messages into the network and interfere with its operation. The need to protect against these types of attacks is so basic that all current WLAN products provide standardized security processes in order to establish confidentiality and integrity control according to IEEE 802.11i.[4]

The IEEE 802.11i standard specifies procedures for key negotiations, data encryption and data verification for transmission of user data within a WLAN. Its support is mandatory in the latest WLAN transmission standards (per IEEE 802.11n), which requires that all current products be equipped with this basic protection, regardless of the device vendor. The architecture applicable to the standard stipulates the individual encryption of each and every wireless data transmission. In order to achieve this, pair-wise encryption keys are present between the communication partners (the session key). In addition, built-in integrity protection ensures that the transmitted data is not only confidential, but also unchanged. As a result, the security goals of confidentiality and integrity are achieved. This ensures that control system data is authentic and attackers cannot extract sensitive data, like passwords, from the data traffic, or inject rogue data packets to alter the operation of the control system.

The manufacturer's association Wi-Fi Alliance[5] has integrated the specified architecture according to IEEE Standard 802.11i into its own procedure known as Wi-Fi Protected Access 2 (WPA2). [See Figure 1] WPA2 includes two modes – Personal and Enterprise – with the main difference involving the mechanism for authentication. Using WPA Personal mode, there is one common password for all WLAN devices in the network (Pre-Shared Key). This password is pre-configured individually for all devices and access points. Such simplistic key management might be practical for very small networks, but the password management creates a big barrier for more complex industrial networks. Typical recurring procedures, such as the replacement of an old key or the exclusion of a lost or stolen WLAN device from a network, usually require a manual and complex reconfiguration of all access points and clients.

The WPA Enterprise mode allows the administrator to assign each device a different key and to manage those keys in a central authentication database (i.e., a RADIUS server). Using the IEEE Standard 802.1x for port-based authentication, the access point can validate every WLAN device individually when a connection is established. It is possible to configure a unique key for every device and to manage it in the database. Thus, passwords can be managed centrally, while lost or stolen devices can be simply disconnected from the network by removing their key information from the database.

Furthermore, advanced WLAN access points allow individual devices to assign different virtual LANs (VLANs) by means of WPA Enterprise, so that devices with different roles can be clearly differentiated.

For example, a WLAN-connected sensor and a WLAN surveillance camera could be isolated from each other by assigning them to different VLANs. This results in the sensor only communicating with the control server, while the camera's communication is limited to sending information to a surveillance terminal. The segmentation makes it difficult for attackers to gain further access to the network should a simpler device be compromised – an example of Defense in Depth. Plus, there is typically no negative impact on the performance of the network so this measure can significantly improve network security, without affecting the speed, throughput or operation of the network and the application.

Maintaining a Robust, Reliable Network

In addition to confidentiality, both robustness and availability play an extremely important role in industrial networks. And while IEEE 802.11i and WPA2 protect against attackers who target data traffic within the industrial network, they only offer limited protection when it comes to robustness and availability.

The management functions of the network, which are controlled by "management frames," are especially vulnerable to forgery and wiretapping. Management frames are network packets that are transmitted wirelessly, like data packets, but instead of containing user data, they serve to organize the internal operation of the network. For example, devices can use management frames to log on and off the network, initiate new key exchanges, and report when they roam from one access point to another.

Unfortunately, WPA2 protection does not include encryption or proof of authenticity for these management frames. Therefore, information about the network can be gained from wiretapped management frames and forged management frames can be sent with a wrong sender identity. As a result, attackers can disrupt the operation of the network.

One example of this would be if an unauthenticated attacker sends a fake management frame to the network and requests an access point to disconnect a WLAN client. Since the access point has no means of detecting that the command came from the attacker and not the victim device, it will execute this order and terminate all communication with the victim WLAN client. Therefore, the quality of connections and the reliability of the whole network can be easily disturbed by faked management frames. This can create major problems for industrial plants because devices become disconnected and connections become unstable, leading to severe malfunctions. In the worst case, this can even lead to a total loss of the operator's control over the entire production process. Not only would the operator's commands not come through, but it could also lock out the true network operator.

To thwart such attacks, a technique called Protected Management Frames (PMF) was introduced in the IEEE 802.11w standard.[6] PMF is a feature that makes it possible to encrypt and protect management frames against forgery. In doing so, the mechanism for authentication and encryption present in WPA2 is extended to achieve the "confidentiality" and "integrity" of the management frames. It then becomes extremely difficult, if not impossible, to misuse the sensible management functions to attack a network. Unfortunately, very few device vendors support this function in the industrial space. It is therefore worthwhile to consider the support for PMF when choosing the products that form the infrastructure for an industrial wireless network solution.

Detecting Attacks and Anomalies

The operations and communication in a network are often not observable by the users. This is especially true in a wireless network design where many processes and activities on the wireless interfaces are performed automatically and are completely invisible, even for network administrators. While this transparency simplifies the use and operation of the network (because the user is not forced to deal with individual operations within the network) it makes it more difficult to recognize attacks and suspicious behavior of users. This is particularly valid for industrial networks that often provide machine-to-machine communication and operate autonomously over long time periods. The absence of insight into the events that take place on the wireless channel (e.g., the use of management frames) allows attacks to remain undetected and makes it harder to take corrective action. For this reason, it is important that a WLAN solution can quickly detect anomalies in the wireless communication before the attacker can affect the operation of the industrial plant.

A Wireless Intrusion Detection System (WIDS) in the access point can detect and report a wide range of suspicious behaviors. For example, it can identify whether an attacker scans for open networks, forges management frames, or tries to impair the network communication by forged authentication messages. In doing so, the WIDS records suspicious behaviors by means of rules and thresholds and informs the user via email, system log message or network management protocols (e.g., by Simple Network Management Protocol (SNMP) traps).

WIDS solutions can either be built into the access points or be added to a network as an additional component. However, when choosing your WLAN and WIDS solution, economic aspects should also be considered. Separate WIDS solutions typically are only cost effective for large enterprise WLAN networks with many access points and clients. When planning small and medium WLAN networks that are often found in the industrial environment, think carefully about what possibilities a WLAN device with an integrated WIDS provides by itself and when a separate WIDS solution justifies an additional investment.

Other attack scenarios are the so-called "rogue" access points, as well as wireless phishing (pronounced "fishing"),

coined wiphishing. In the first scenario, unsanctioned or even malicious access points provide "nearly identical" wireless services in the proximity of an industrial network. A rogue access point provides unsanctioned and potentially insecure access from inside the network. For example, an employee who would like to use private wireless devices may choose to connect his own (and potentially insecure) access point to the wired network, effectively creating an uncontrolled entry point for attackers.

Wiphishing takes the use of unsanctioned access points even one step further. An attacker who performs a wiphishing attack establishes an individual access point near the WLAN network in order to lure WLAN clients into this fake network. In the process, the fake access point uses the same network name, or service set identifier (SSID), as the industrial network, but often without password protection so that all clients connect themselves erroneously to the forged network. Due to the identical WLAN names, it is difficult for staff and service personnel to recognize whether a mobile device or a WLAN device on the site is connected to the correct network. When a WLAN device is connected erroneously to the fake access point it may disclose sensitive data or internal information regarding the structure of the industrial network. A potential attack scenario would be the phishing of access data for individual staff. If the WLAN client communicates only with the Internet, even classic "man-in-the-middle" attacks are possible and often remain undetected.

Both attacks and weaknesses (rogue access points and wiphishing) stem from the same problem: insufficient awareness of the wireless environment of a network. Without active monitoring, the environment of a wireless network remains largely invisible until actual problems in the applications appear. To thwart these problems early on, operators must gain complete oversight of other networks in the environment of the site. Therefore, a comprehensive, secure and reliable WLAN solution should provide rogue access point detection and wireless environment visualization. With this information, the legitimate access points within the network can identify if an unknown device uses the network's SSID or if a new and unknown access point appears.

Communicating Between WLAN Devices Via Ethernet

It is rarely sufficient to only consider external attackers. Often, attacks occur from the inside of a network. Even the most effective WLAN encryption does not offer protection when the attacker is an insider or gains access to a network by some other means (e.g., by viruses or phishing attacks). Consistent with the principles of Defense in Depth, it is important to establish barriers that deter internal attackers from extending their influence by compromising other systems in the network.

As soon as a client device has been integrated into a WLAN, it can communicate with other devices in the same network or

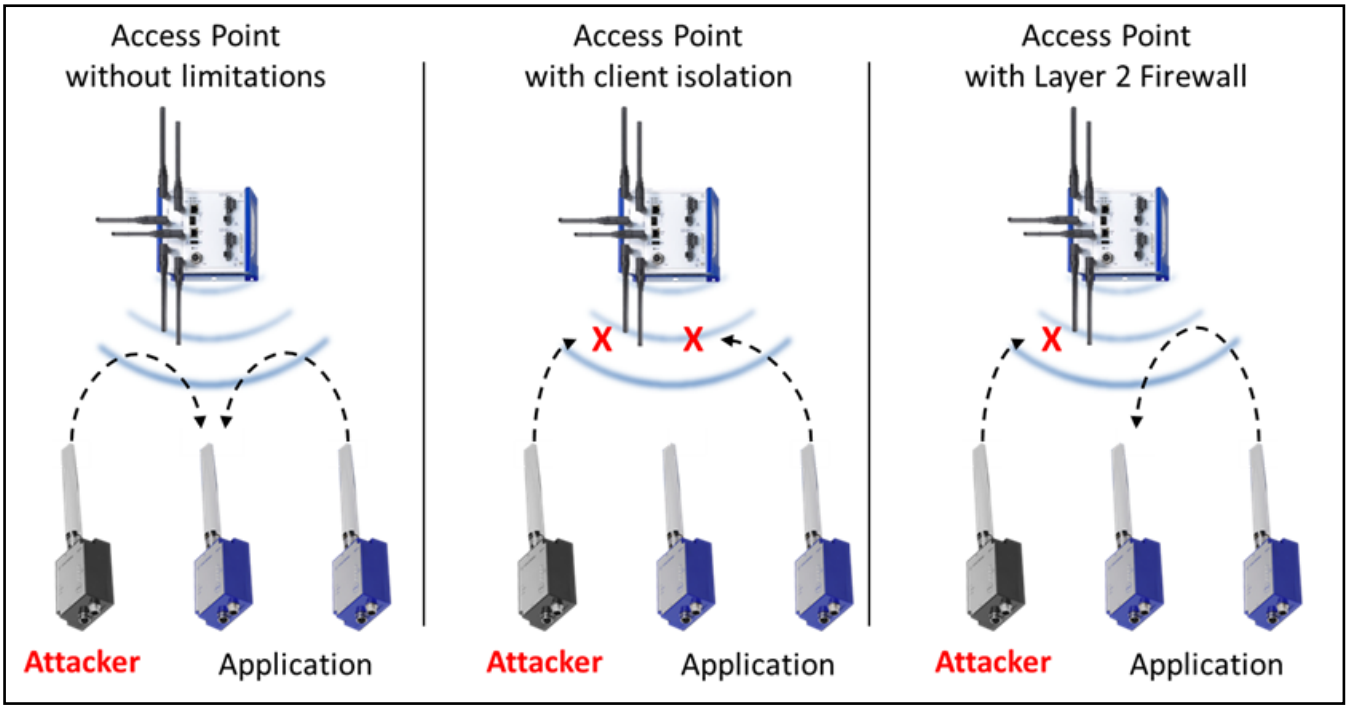

Figure 2: Different mechanisms to prevent client-to client communication allow for different granularities. Client isolation can only block all or no traffic between all clients. A Layer 2 firewall can selectively restrict the communication between clients.

subnetwork. This means an attacker can use the network to infiltrate additional network systems to extend his influence. This problem can only be solved by selectively limiting communication to the minimum that is required to run the industrial application.

Many wireless access points can suppress all communication between all connected clients, thereby isolating all clients from one another. This simple method to suppress all client-to-client communication effectively protects all clients from each other. However, while this approach can work well in enterprise applications, it is often not applicable for industrial networks because the connected WLAN clients may have to directly relay information in order to operate and monitor plants.

For example, a control panel that is connected via WLAN may directly communicate to a sensor that is also connected to the WLAN. Therefore, for sophisticated industrial applications, it is necessary to provide more fine-grained barriers in order to allow desired communications while blocking all undesired communication. Such fine-grained limitations can be implemented with a configurable firewall on the Ethernet level (Layer 2 firewall). This type of firewall can selectively filter the traffic between WLAN clients and limit the allowed traffic to specific peers or protocols. In contrast to using a VLAN configuration, a Layer 2 firewall is more selective because it allows segregating devices into different groups where communication is allowed, as well as enabling finer and more flexible control on a per protocol basis.

As industrial applications often operate within an Ethernet network without routing, it is important that networks explicitly support a Layer 2 firewall that can filter traffic between WLAN clients. Many

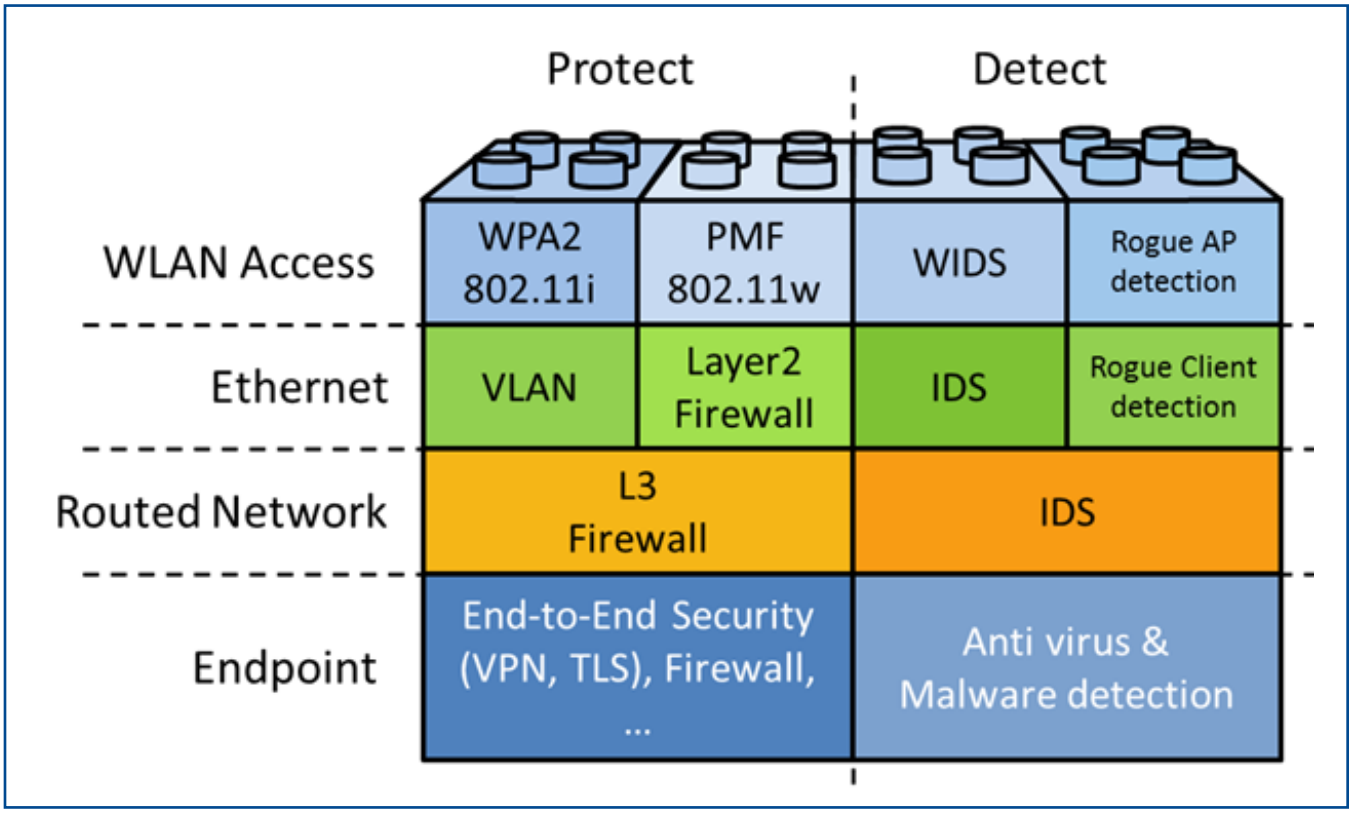

Figure 3: The complete construction kit for WLAN security. The endpoints of elements are described only in parts and as an example.

products, however, only provide firewalls for routed traffic that is relayed across network boundaries. These Layer 3 firewalls always allow directly switched/bridged traffic to pass and offer little to no protection for the communication between WLAN clients, or even wired clients on the same network.

Additionally, an Intrusion Detection System (IDS) for Ethernet traffic can identify clients who show erroneous, suspicious or unusual behavior. Thus, an attack from the inside of the network can be recognized and recorded. A special procedure to identify attacks or anomalies within a WLAN network is the detection of "rogue clients" – unknown and unsanctioned clients that associate themselves to the network. New and unwanted devices can be a sign of an attacker who successfully acquired a WLAN key. Detection and timely notification of rogue clients allows the administrator to identify modifications within the WLAN and quickly take appropriate actions.

Protecting Network Boundaries with Firewalls and IDS

Industrial plants may be physically distributed over wide areas and may contain a wide range of interconnected applications and machines. According to Defense in Depth, individual areas of the network in a connected plant must be sealed off from one another so that an attacker who gains access to one area cannot harm the complete network. An access point often takes a central position in the network by wirelessly connecting clients to the routed network or by connecting multiple distant sites through wireless point-to-point links. Because of this central position in the network, the access point or access point controller is an excellent device to selectively enforce the isolation of the different devices and networks by providing firewalling functionality.

A firewall can model and enforce desired or undesired network communications. Stateful packet inspection can restrict the possible communication to certain communication peers, communication protocols and even to certain protocol behaviors. In doing so, logical relations between the devices belonging to an industrial application can be modeled and enforced. Similar to the previous example of the sensor and the control panel, such relations can also be enforced across network boundaries for routed traffic.

Industrial networks are mostly purpose-built and experience little change. Violations of firewall rules (e.g., if the sensor suddenly starts to talk to other systems or performs port scans) become strong and reliable indicators of an attempted attack or malfunctioning equipment. An IDS for non-wireless network traffic linked with a Layer 3 firewall can help detect and thwart attempted attacks by making the administrators aware of the situation quickly. A violated firewall rule can trigger warning messages or emails to the administrator so that the network operator can quickly learn about misbehaving and dangerous devices.

Figure 3 shows the complete picture of the discussed security functions grouped in their different functions and communication layers. The figure also depicts the endpoints – the devices that actually run the industrial applications. In addition to the described industrial network security measures, in some cases, the endpoints of the communication can also be protected. However, the set of available security controls largely depends on the nature and type of the endpoint. In some cases, the endpoints are industrial PCs that offer a wide range of possibilities to improve security. In other cases, the endpoints are embedded systems without any option to enable additional security functions. Hence, a comprehensive, reliable security strategy cannot solely rely on endpoint security, but must take precautions on each layer of the network as well.

Available ICS Security Functions

The described features and methods are available with all Hirschmann OpenBAT Access Points and from software version 9.0 of the HiLCOS wireless operating system. With HiLCOS, Belden offers an exceptionally rich portfolio of security features, including IEEE 802.11i, RADUS Authenticator and Server, IEEE 802.11w, Wireless Intrusion Detection System, Layer 2 and Layer 3 firewalls, as well as rogue client and access point detection. These features are all available and can be deployed in small, medium and large networks without additional third-party products.

Summary

As this white paper has demonstrated, the options for securing WLAN networks are very diverse. Every described feature, however, serves a specific purpose. Thus, despite the complexity of the topic, the combination of these features and functions results in an organized construction kit rather than a patchwork of protection measures. When these features are combined in a single device, they create a flexible and powerful security tool. In addition, due to the independent nature of these elements, their application creates multiple layers of protection in order to implement effective security concepts, as in the highly effective Defense in Depth threat mitigation strategy.

HIRSCHMANN
A BELDEN BRAND

References

1 Belden blog. "Cyber Security for Industrial Applications: Defense-in-Depth." http://www.belden.com/blog/industrialethernet/Cyber-Security-for-Industrial-Applications-Defense-in-Depth.cfm

2 Federal Office for Information Security, Bundesamt für Sicherheit in der Informationstechnik – BSI, The State of IT Security in Germany 2014, 2014 https://www.bsi.bund.de/EN/Publications/SecuritySituation/SecuritySituation_node.html

3 OSI Reference Model (Open Systems Interconnection), TechTarget.com. http://searchnetworking.techtarget.com/definition/OSI

4 + 6 Institute of Electrical and Electronics Engineers, Inc., Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications (ANSI/IEEE Std 802.11, 2012 Edition (802.11-2012)), 2012

5 Wi-Fi Alliance. http://www.wi-fi.org/

About Belden

Belden Inc., a global leader in high quality, end-to-end signal transmission solutions, delivers a comprehensive product portfolio designed to meet the mission-critical network infrastructure needs of industrial, enterprise and broadcast markets. With innovative solutions targeted at reliable and secure transmission of rapidly growing amounts of data, audio and video needed for today's applications, Belden is at the center of the global transformation to a connected world. Founded in 1902, the company is headquartered in St. Louis, USA, and has manufacturing capabilities in North and South America, Europe and Asia.

For more information, visit us at www.beldensolutions.com and follow us on Twitter @BeldenInc.

Phone: **1-855-400-9071**