Securing WLANs using 802.11i

Draft Recommended Practice

February 2007

Securing WLANs using 802.11i
Draft

Author: Ken Masica, Lawrence Livermore National Laboratory
February 2007

for
Idaho National Laboratory Critical Infrastructure Protection Center
Idaho Falls, Idaho 83415

Prepared by
Lawrence Livermore National Laboratory

LAWRENCE
LIVERMORE
NATIONAL
LABORATORY

Recommended Practices Guide Securing WLANs using 802.11i

Ken Masica

Vulnerability & Risk Assessment Program (VRAP)
Lawrence Livermore National Laboratory (LLNL)

for
DHS US CERT
Control Systems Security Program (CSSP)

October 2006

This work was performed under the auspices of the U.S. Department of Energy by University of California, Lawrence Livermore National Laboratory under Contract W-7405-Eng-48.

UCRL-TR-225541

Table of Contents

A. Introduction

This paper addresses design principles and best practices regarding the secure implementation and operation of Wireless LAN (WLAN) communication networks based on the IEEE 802.11 protocol. First, a general overview of WLAN technology and the 802.11 standard is provided. The subsequent sections describe the various initial and interim IEEE security standards leading to the 802.11i standard. An explanation of the 802.11i standard for securing WLAN networks is then presented, followed by principles for designing secure WLAN networks, and a list of specific security best practices that can be used as a guideline for organizations considering the deployment of a WLAN. Finally, a section on technical issues and special considerations for installations of WLAN networks in industrial environments is presented. A concluding section summarizes key points and is followed by a list of online technical references related to the topics presented.

B. Technology Background

WLAN technology is a form of wireless ethernet networking standardized by the IEEE 802.11 Working Group (WG). There are a series of 802.11 standards that have been produced since the formation of the WG in 1990. The goal of the 802.11 WG was to create a set of standards for WLAN operation in the unlicensed portion of the *Industrial, Scientific, and Medical* (ISM) frequency spectrum. (The ISM bands are ranges of frequencies set aside by the FCC for unlicensed, low-power operations.) See **Table-1** below for a list of the frequencies and data rates defined by the IEEE 802.11 WG for WLAN networks in the chronological order in which they were created.

IEEE Standard	Year Released	Maximum Data Rate	ISM Frequency Band	Modulation Type
802.11	1997	2 Mb/s	2.4GHz & IR	FHSS, DSSS, & IR
802.11b	1999	11 Mb/s	2.4 GHz	DSSS
802.11a	1999	54 Mb/s	5.0 GHz	Orthogonal FDM
802.11g	2003	54 Mb/s	2.4 GHz	Orthogonal FDM

Table-1: *WLAN frequencies, data rates, and modulation*

The areas standardized by the IEEE 802.11 WG fall within the first and second layers of the OSI Seven Layer Model -- referred to as the Physical and Data Link Layers, respectively. **Figure-1** below shows a graphical representation of how the IEEE 802.11 protocol layers map to the OSI seven layer model. As with traditional wired ethernet networks based on the IEEE 802.3 standard, the Data Link Layer is subdivided into the Logical Link Control (LLC) and Media Access Control (MAC) sublayers. An existing IEEE 802 series protocol, 802.2, was adopted for use with WLAN networks for the LLC layer. A new MAC sub layer for 802.11 was then developed, based on *Carrier Sense Multiple Access with Collision Avoidance* (CSMA/CA) channel access methods. The 802.11 MAC serves as a single, common interface to the Physical Layer (PHY) protocols below it. Four different PHY standards have been developed to date as shown above in **Table-1**. The PHY layer is responsible for the actual Radio Frequency (RF) transmission and defines the frequencies and the modulation methods used. It is worth noting that the very first PHY developed, the original 802.11 PHY, suffered from low throughput and interoperability problems and was not widely adopted. Subsequent PHY standards (802.11a/b/g) based on better modulation techniques and higher throughput were developed to address the problem and are now in wide use. Although the initial problems with the original 802.11 Physical Layer specification delayed the wide-spread adoption of WLANs, it did spur the creation of the Wireless Ethernet Compatibility Alliance (WECA), an industry group devoted to the certification of 802.11 products for standards compliance and interoperability with other WLAN products. WECA brands compliant WLAN products with the “Wi-Fi” (for *Wireless Fidelity*) label, so WLAN networks are often referred to as *Wi-Fi* networks.

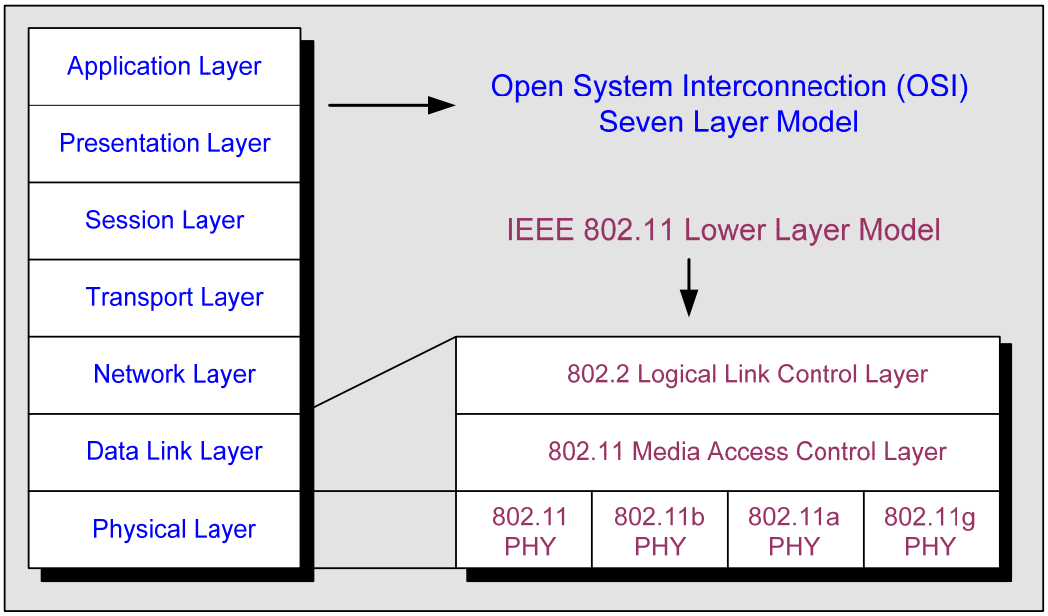

Figure-1: *Corresponding OSI and IEEE layered models*

C. Operational Modes

In general, 802.11 networks can be configured to operate in three different modes or topologies:

1) *Infrastructure Mode*: This is the most common WLAN configuration that allows one or more client stations to communicate wirelessly with an Access Point (AP). In IEEE terminology, this is considered a Basic Service Set (BSS) in which the AP coordinates all activities among stations (such as all associations and disassociations with clients). The BSS is defined by the Service Set Identifier (SSID), which is a unique ID that identifies the WLAN. AP's may send out beacons that broadcast the SSID so that nearby stations can attempt to establish an association and join the WLAN. (SSID broadcast is not recommended from a security standpoint; this will be discussed later in more detail.) The AP accepts traffic from stations that have successfully authenticated and established an association with the WLAN. The AP normally passes frames between the WLAN and a wired network to which it is connected (the *distribution system* in IEEE parlance). It can also pass frames between WLAN stations if configured to do so. (This is also generally not recommended from a security standpoint unless it is required by the application.) **Figure-2** below shows a conceptual example of a WLAN operating in infrastructure mode.

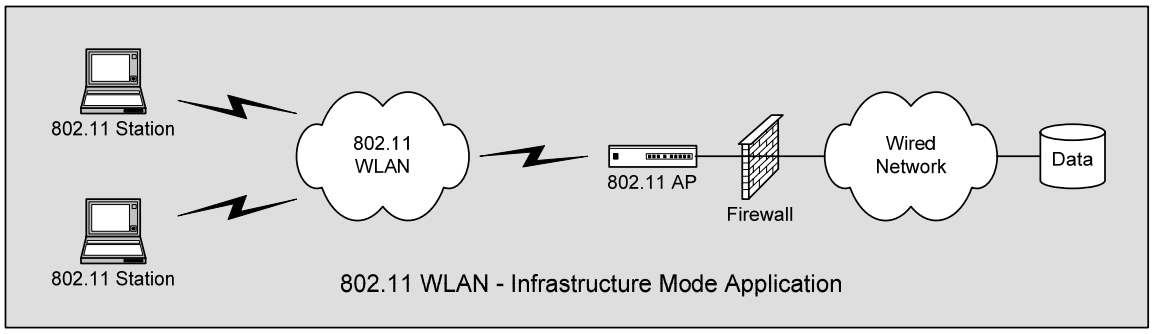

Figure-2: *WLAN Operating in Infrastructure Mode*

2) *Ad Hoc Mode*: This mode involves the direct wireless communication between two stations as depicted in **Figure-3** below. In IEEE terminology, this is referred to as the formation of an Independent Basic Service Set (IBSS). An Ad Hoc WLAN does not scale like an infrastructure mode WLAN, and from a security standpoint, Ad Hoc capability should be disabled in client stations unless it is an absolute requirement of the application.

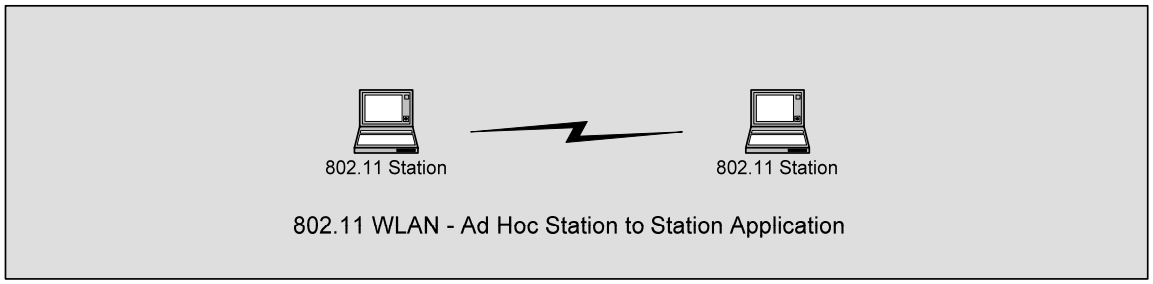

Figure-3: *WLAN Operating in Ad Hoc Mode*

3) *Bridging Mode*: Often, an 802.11 network is used as a bridge between two other networks. This can be an inexpensive way of establishing a link between two network segments when installing a wired connection is costly or prohibitive for some reason. In a bridging application, the access points establish an association with each other and act as a bridge to pass traffic. Often, this configuration is used to bridge two wired network segments, but it could also be used to bridge other wireless networks or applications, such as a low-power 802.15.4 network in which the nodes are located remotely and must communicate back to the plant network. **Figure-4** below depicts the bridging mode.

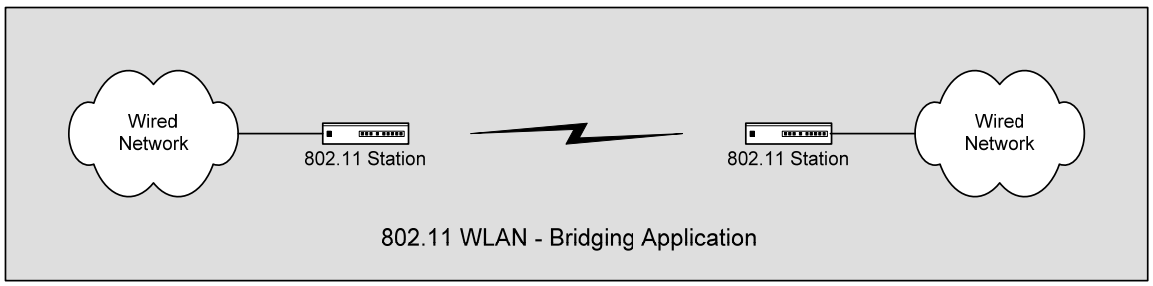

Figure-4: *WLAN Operating in Bridging Mode*

D. WEP Security

Security in the original 802.11 standard produced by the IEEE in 1990 was referred to as *Wired Equivalent Privacy* (WEP). WEP was based on the use of the same shared private encryption key (or limited set of rotating keys) among all stations on a WLAN. This meant that if the key from a single station was compromised, the entire WLAN encryption scheme was compromised. Also, a weakness in how WEP was implemented allowed it to be cracked by public domain tools (e.g. WepAttack, AirCrack, etc.) by an attacker capturing packets passively. Furthermore, the flawed implementation also meant that increasing the key size from the available 40-bit exportable or 104-bit domestic options did not increase the difficulty in breaking the key *exponentially*, only *linearly*. Thus, simply increasing the key size was not an effective way to improve security. These weaknesses, combined with the lack of key management for distributing and updating keys on all WLAN stations and access points, made WEP security inadequate for protecting wireless networks and difficult to manage. In response, organizations often turned to other security solutions, such as Layer-3 VPN (Virtual Private Network) encryption in order to provide security. However, such Layer-3 solutions did not provide security (authentication and encryption) at the Layer-2 ethernet frame level, could be costly to implement, and posed potential problems when mobile devices roamed between access points. Furthermore, VPN client software was not always available for WLAN station devices used in industrial applications (such as some bar code scanners, PDAs, sensors, and instruments).

E. WPA Security

Once the weaknesses of WEP became apparent, the IEEE began work on a security standard to serve as a replacement for WEP. The new standard was referred to as the 802.11i standard. The Working Group's approach was to develop a relatively quick solution for existing legacy equipment (access points and client adapters) that customers could implement with software or firmware upgrades from their vendors. The 802.11i Working Group would also then develop a strong, standards-based encryption solution that would require new hardware but could be incorporated into future WLAN products.

In 2003, the Wireless Ethernet Compatibility Alliance (WECA) standardized on an interim security solution based on the initial work of the 802.11i group and referred to it as *Wi-Fi Protected Access* (WPA). WPA was a subset of the capabilities that were to be part of the final 802.11i standard that could be brought to market while the final version of the standard was being completed.

The WPA solution addressed two critical shortfalls of the original WEP-based security standard:

a) Design weakness in the WEP protocol.
b) Lack of an effective key distribution method.

To address these shortfalls, WPA incorporated two protocols of the 802.11i standard:

1) *Temporal Key Integrity Protocol (TKIP)*: This protocol fixed problems with frame encryption and integrity of WEP. The TKIP protocol uses the original RC4 encryption algorithm that was also used by WEP but adds a mixing function that creates per-frame keys to avoid the weak-key attacks on WEP. It also adds a message integrity code (MIC) which enables devices to authenticate the packets they receive. TKIP was designed to run on most existing WLAN station and access point equipment with only software/firmware upgrades.

2) *802.1x Port Based Authentication*: This protocol was an existing IEEE standard adapted by the 802.11i Working Group and incorporated into the interim WPA solution. It is referred to as port based authentication because it was designed to provide a framework that allows a device connecting to a network (wired or wireless) to first be authenticated before being granted access. 802.1x allows for mutual authentication, meaning both the client station can be authenticated before being granted admission to the WLAN and the client can authenticate the WLAN before joining. (The latter authentication capability is important to prevent rogue access point attacks, where an attacker operates an unauthorized access point in the vicinity of the WLAN and attempts to have clients connect to it in order to capture login information and other data from the client.) 802.1x also provides a key distribution mechanism since it provides a framework for the secure delivery of keying material once a client has been authenticated.

The two key components of WPA, TKIP and 802.1x, addressed the primary problems with the original 802.11 security model based on WEP. They were software-based solutions that were the first components of the 802.11i standard that was being developed to provide a strong frame encryption and authentication replacement for WEP.

F. 802.11i Security

The final 802.11i WLAN security standard was ratified by the IEEE in June of 2004. The standard is backward compatible with WPA and includes the TKIP and 802.1x protocols. Additionally, a stronger frame encryption and authentication alternative was added that could be incorporated into new hardware from vendors. The new cryptography was based on the AES (Advanced Encryption Standard) algorithm that was selected by NIST and adopted by the U.S. government as a national standard and replacement for the previous standard based on the DES (Data Encryption Standard) algorithm. Strong, standards-based AES encryption and authentication was the primary component added to finalize the 802.11i standard.

Two additional but less prominent features, *key caching* and *pre-authentication*, were also added to the standard to enable fast and secure roaming. Key caching stores information about the client on the network so that if a station leaves an access point and returns, credentials for re-authentication do not have to be entered again (subject to configured session timeouts). Pre-authentication refers to the ability of a network to send authentication data between access points so that a roaming station does not need to authenticate to each access point. These features of 802.11i enhance mobile WLAN

applications over a larger scale among multiple access points, such as a technician with a hand-held device roaming throughout a plant or a device such as an overhead crane or a transportation vehicle transmitting position information.

The AES implementation developed for 802.11i is referred to as the *Counter-Mode/CBC-MAC Protocol* (CCMP). It uses the AED algorithm in two different modes to provide frame confidentiality), authentication, and integrity. For confidentiality, the AES algorithm is used in Counter Mode. For authentication and integrity, the AES algorithm is used in Cipher Block Chaining Message Authentication Code (CBC-MAC) mode.

It should also be noted that CCMP protects fields of the frame that are not encrypted, such as the source and destination Ethernet addresses. Portions of the 802.11 frame that are not encrypted but protected by CCMP integrity are referred to as *Additional Authentication Data* (AAD). Authenticating the source and destination MAC addresses of the frame protect against spoofing attacks and the replay of captured packets to different destinations. (AAD protection is an example one of the advantages of using 802.11i and Layer-2 level security for WLAN networks, compared to a Layer-3 only solution.)

G. WPA2 Security

Once 802.11i was ratified, the WECA developed an interoperable implementation of the standard in September 2004 called WPA2 that could be used to test WLAN products for compliance. The two terms, 802.11i and WPA2, are used synonymously to mean the new security standard for 802.11 networks. WLAN products that have been tested and certified for 802.11i compliance are branded with the WPA2 label.

H. Six Security Design Principles

This section describes the principles involved in architecting and designing a secure WLAN solution. These principles should be employed in the WLAN planning and design phase. The subsequent section will list specific best practice guidelines for the implementation phase of the WLAN.

The following are design principles for developing secure WLAN architectures:

1) Principle: *Apply a Defense-in-Depth approach.*

   This concept of secure design involves implementing multiple layers of security measures to control access to mission-critical systems and networks. These are often the targets that an attacker attempts to gain unauthorized access to by compromising a WLAN and using it as an attack path or vector into an organizational network such as a plant network where the target systems reside. In order to defend the target environment, multiple security measures should be implemented so that if that one measure is defeated by an attacker, additional measures and layers of security remain to protect the target environment. Measures such as separation of wireless and wired network segments, strong device and user authentication methods, filtering of traffic

based on addresses and protocols, securing end-points/stations from unauthorized access, and monitoring and intrusion detection on the wireless and wired segments are examples of multiple layers of defense that can be employed to achieve a defense-in-depth design.

2) Principle: *Separate and segment the WLAN from the wired LAN.*

   WLAN(s) and wired networks should not be directly connected. So, for example, a non-critical ISA Class 4 or 5 wireless environmental monitoring and logging WLAN network should not have direct connectivity to the wired plant network, but instead be separated by a device such as a firewall, bastion host, or security gateway to provide segmentation and control of traffic.

3) Principle: *Require mutually authenticated access to the WLAN for all users and devices.*

   All devices and users that access the WLAN should be authenticated before access is provided. Additionally, the device or user should also authenticate the WLAN to ensure it is legitimate and not a rogue network setup by an attacker. WLAN technology, often by default, allows "open" authentication in which no credentials are required for a device to access the WLAN. Obviously, this type of access is not secure and should be avoided in favor of stronger mutual authentication based on the 802.1x protocol defined in the 802.11i standard.

4) Principle: *Protect WLAN traffic by implementing strong security at the Layer-2 level.*

   As previously discussed, the 802.11i/WPA2 standard provides Layer-2 encryption, authentication, and integrity of WLAN Ethernet frames and their payloads. AES is the stronger, more desirable security solution than TKIP, but typically must be implemented in hardware. TKIP can be used to upgrade existing or legacy WLAN equipment. The original WEP security standard should not be used for securing Layer-2 traffic.

5) Principle: *Restrict traffic between the WLAN and the wired network.*

   The applications, protocols and source/destination communication pairs should be restricted to the minimum required to support functional requirements. Basic ethernet MAC address filtering at Layer-2 can be implemented in most access points to permit only known and authorized devices to be forwarded by the access point. At the IP level, a firewall separating the WLAN and wired LAN can filter on IP source and destination address and specific application and service ports. The most restrictive rulesets should be developed for the firewall, and a "default deny" configuration should be implemented that allows only the required application traffic between source and destination pairs.

6) Principle: *Monitor the WLAN to detect intrusion attempts.*

   Intrusion Detection Systems (IDS) monitor network traffic and attempt to identify potential attacks based on known signatures, traffic patterns, or anomalies from baseline activity. There are a variety of Wireless IDS (WIDS) products available

commercially as well as some that are public domain. WIDS products can be dedicated, stand-alone systems or capabilities integrated into the access points that provide the WLAN network access. Ideally, capabilities for alarm generation and centralized logging should also be implemented.

Shown below in **Figure-5** is a conceptual example of the WLAN design principles. It shows several WLANs operating in an industrial environment that are segmented from each other and from the plant network using dedicated ports on a multi-port firewall. The access point should provide Layer-2 filtering on authorized MAC addresses and it should not allow traffic between WLANs. A separate network segment for security services (such as 802.1x authentication and IDS alerting) and security administration is shown to emphasize the importance of controlling configuration access to the devices on the network. An IDS for both the wired and wireless networks is used to monitor suspicious activity and alert on potential attacks. The WLAN network segments shown are running example wireless applications in an industrial environment. Two bridging WLANs are shown, one that bridges a low-power wireless mesh network and the other a wired network. A WLAN for mobile technician access is also shown as part of the example.

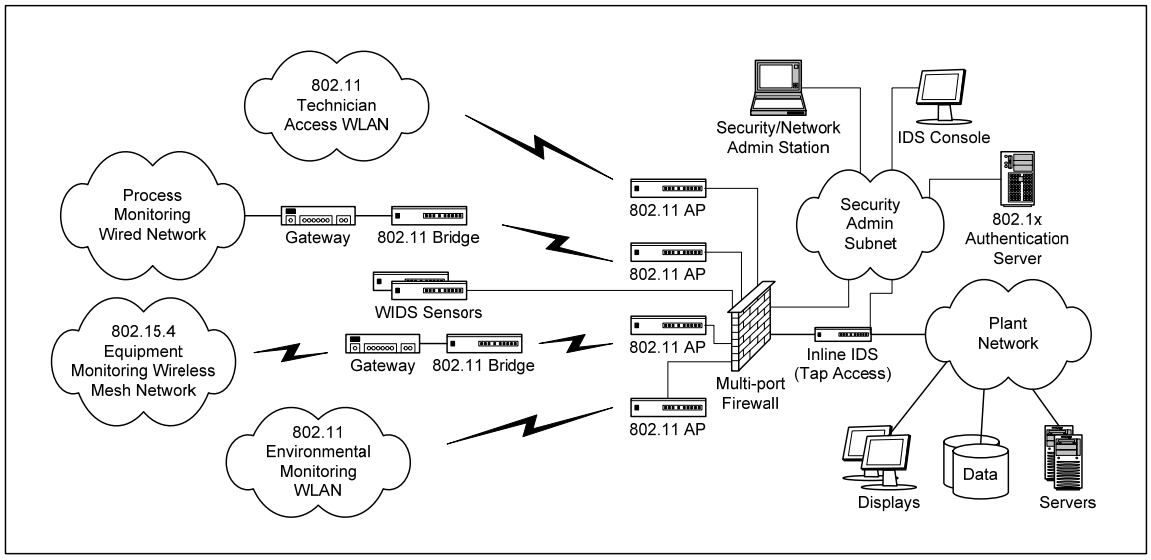

Figure-5: *Example of an industrial environment employing principles of secure WLAN design*

I. Sixteen Security Recommended Practices

The following are recommended practices that should be considered when implementing an 802.11 WLAN:

1) Recommendation: *Create a WLAN security policy.*

The organization should develop a strong WLAN security policy and educate all employees regarding the policy. The policy should outline a framework for the development of installation, protection, management, and usage procedures. All

mission-critical assets and control components should be identified. Security and operational guidelines, standards, and personnel roles should be defined.

2) Recommendation: *Do not rely on default security configurations of WLAN access points and adapters.*

   In general, WLAN equipment ships with minimum security features and controls enabled. For example, access point equipment will often ship in "Open Authentication" mode by default, meaning that no method of authentication between the stations and the access point is needed for the stations to establish an association (connection) to the WLAN network. Under open authentication, stations simply join the WLAN without restriction.

3) Recommendation: *Employ MAC address filtering on the access points.*

   This is a low-level security control on the access point that permits only those stations with ethernet MAC sub layer addresses on a list contained within the access point to communicate with the access point.

4) Recommendation: *Disable SSID beacon transmissions.*

   Access points in most cases will by default broadcast a "Service Set Identifier", or SSID. This is essentially the name of the WLAN that a client station will use to identify a WLAN in its environment. For security purposes, it is best to disable SSID broadcast beacons so that the WLAN is not advertised to client stations that should not be allowed to connect. When the SSID broadcast is disabled, the client stations must know the SSID of the WLAN to which they want to connect. Suppressing the SSID beacon, although a minor security measure, ensures that an organization's WLAN networks, especially control system networks, are not announced or easily known.

5) Recommendation: *Use non-suggestive SSID naming conventions.*

   Because SSID's serve as the name of WLAN networks, organizations will often name them according to their function or consistent with the unit of the organization that deployed it (for example, "ABC Corp", "Chlorinator", or "SCADA Dept"). It is best to not suggest the function or organization, if possible, in the SSID. It is best to not aid an attacker collecting reconnaissance information on a WLAN installation with use of a sniffer by providing the function or purpose of the network, especially if it pertains to industrial applications.

6) Recommendation: *Utilize 802.11i security, not WEP, for Layer-2 security.*

   The 802.11i/WPA2 standard employs both TKIP and AES to provide stronger frame encryption, authentication, and integrity and replaces the original WEP standard. TKIP, although not as strong as AES, can be used on legacy equipment to quickly address the weaknesses of WEP through software/firmware upgrades to existing WLAN access points and adapters. AES is the stronger and more secure option that

should be used or migrated to if possible, especially since FIPS-compliant products based on AES are available.

7) Recommendation: *Unless absolutely needed, disable direct station-to-station "Ad Hoc Mode" transmission.*

   "Ad Hoc" mode enables stations to communicate with each other directly. Unless an industrial application requires this type of communication, it should be disabled so that a potential attacker cannot try to associate directly with a station on the WLAN.

8) Recommendation: *Unless absolutely needed, disable station-to-station communication through the access point.*

   As discussed previously, in "Infrastructure Mode" of WLAN operation, stations communicate with one or more access points, which coordinate all activity on the WLAN. (See **Figure-2**). The normal traffic pattern is communication between wireless stations on the WLAN and host systems or servers on the wired network behind the access point (such as a data logger or database). If communication between WLAN stations through the access point is not needed to support functional requirements, it should be disabled in the access point(s). Allowing this traffic pattern when it is not needed could allow an intruder who gains unauthorized access to the WLAN to launch attacks against potentially vulnerable WLAN clients.

9) Recommendation: *Protect the WLAN end-points and stations (especially in mobile applications) through technical and administrative hardening methods such as the following:*

   a) Remove or disable unnecessary services.

   b) Remove or disable unnecessary user and service accounts.

   c) Disable network bridging in devices that support it.

   d) Disable or restrict management protocols such as SNMP.

   e) Enable wireless threshold parameters, such as inactivity timeouts and maximum supported associations.

   f) Disable split tunneling option if a Layer-3 VPN is used.

   g) Protect running software with the latest (and tested) patch levels.

   h) Scan end-points periodically to test for proper security configuration and potential vulnerabilities.

   i) Install anti-virus and anti-spyware tools if the end-point can support it.

   j) Use a filtering device such as a personal firewall if the end-point can support it. If the end-point is not a general purpose computer or does not have a computer front-end (such as sensors, scanners, instruments, etc.) then a small, inexpensive

firewall appliance placed in front of the end point to inspect and restrict connectivity to the minimum set of trusted host pairs should be considered.

10) Recommendation: *Employ static IP addressing of devices on the WLAN instead of dynamic assignment if possible when IP is the next higher-layer network protocol.*

Using a static IP addressing scheme for WLAN stations and devices will enable better control, activity tracking, and monitoring of authorized devices on the WLAN. By assigning static IP addresses to devices, security and network administrators can define device-specific access rules in downstream firewalls and routers that connect to the wired network. They can also better track and log activity of devices by permanent IP address compared to dynamic assignment in which address can change for individual devices. Many wireless and wired intrusion detection systems are also more effective when they operate in static IP address environments. Also, in general, it is best to reduce to a minimum the number of network services running in a network environment, so disabling Dynamic Host Configuration Protocol (DHCP) is consistent with this recommendation.

11) Recommendation: *Use static ARP entries on WLAN stations and access points.*

The Address Resolution Protocol (ARP) is used by stations on a network to obtain the hardware (ethernet) address corresponding to an IP address. Normally, ARP entries that translate between the ethernet and IP addresses for hosts on a network are kept in memory before a time-out interval is reached and the cache expires. The normal operation of dynamic ARP is potentially susceptible to ARP poisoning attacks in which an unauthorized machine of an attacker attempts to redirect IP packets to itself be sending bogus ARP responses to hosts on the WLAN so they incorrectly associate a legitimate IP address with an attacker's Ethernet address. In this way, WLAN packets can be erroneously sent to an attacker's Ethernet hardware address. Static ARP entries on the WLAN stations can prevent this type of attack. Static ARP management can be time consuming if the WLAN is large, but if previous recommendations are followed and station-to-station communication is not required and therefore disabled, then the number ARP entries for any given WLAN station should be minimal.

12) Recommendation: *Limit RF power transmission to minimum required levels.*

Wireless signals by their nature cannot generally be contained because Radio Frequency (RF) transmissions propagate through building interiors, through walls, and beyond the operating range of WLAN stations. However, limiting the transmit power levels of station adapter cards and access points to the minimum level required to achieve the coverage and data rates required is a sound security practice. Most access points will have adjustable power level settings, and testing for minimum required signal strength can reduce the detectable transmission distance beyond the industrial environment. This has the benefit of making the WLAN more difficult to detect by "war drivers" searching for WLAN installations.

13) Recommendation: *Use directional antennas if possible.*

As mentioned previously, it is difficult and usually impractical to attempt to control the propagation of RF signals. The RF energy will typically propagate beyond the area in which the stations operate. Another measure in addition to power limiting transmission levels is to use directional antennas on the access points. By default, most access points come with omni directional antennas that radiate the RF signal spherically with equal strength in all directions. Use of directional antennas can channel the RF energy in a particular direction or pattern, such as a sector antenna that radiates the signal in a 30-degree outward pattern. Because of the popularity of 802.11 networks, numerous vendors sell a variety of directional antennas for the 2.4Ghz and 5GHz frequencies ranges. It is important to purchase access points that have detachable or "connectorized" antennas so that the original omni directional antenna can be replaced by a directional antenna.

14) Recommendation: *Deploy or leverage existing wireless intrusion detection capability.*

Similar in concept to a traditional wired intrusion detection system (IDS), a wireless IDS (WIDS) can monitor the WLAN environment and potentially detect attempted known attacks. Several vendors sell stand-alone WIDS solutions with 802.11 sensors that act independently of the deployed WLAN. Increasingly, however, 802.11 technology vendors are incorporating attack detection capability into their product offerings. (Similar to how firewall systems increasingly provide some degree of inline IDS capability as a feature.) The flexibility and range of capabilities in a dedicated stand-alone WIDS should be weighed against the additional cost and complexity of implementation. On the other hand, looking for basic WIDS attack detection capability in WLAN access point offerings when making an initial purchase or upgrading an existing implementation can be an effective way to add this security capability.

15) Recommendation: *If the IP protocol is used as the network layer protocol, employ a private IP addressing scheme.*

Using private IP addressing for the WLAN provides a degree of anonymity in the event that an attacker can obtain the IP addressing scheme. If publicly-assigned IP addresses of the organization are extended out to the WLAN, an attacker can perform a look-up of the organization or service provider that is assigned the addresses. (This may be the block IP addresses assigned to the ISP service provider or it may be the addresses directly assigned to the organization.) This practice also provides a degree of separation and distinction for the WLAN traffic that is propagating on the outside of the trusted wired network infrastructure of the organization.

16) Recommendation: *Ensure that ARP broadcasts from the wired network do not propagate to the WLAN.*

In general, ARP broadcast packets from the wired network(s) should not propagate to the WLAN side since they could reveal Ethernet MAC addresses to an attacker for systems on the wired network side. Using the principle of segmentation, the WLAN and wired LAN networks should be in different subnets and broadcast domains as well as isolated and separated with a filtering device such as a firewall.

J. Considerations for Industrial Environments

This final section discusses issues specific to industrial environments that should be considered when implementing and securing WLAN networks.

1) *Interference*: As discussed previously and shown in **Table-1**, WLANs operate in the 2.4GHz (802.11b/g) and 5GHz (802.11a) frequency ranges. Because industrial machinery environments can produce a significant amount of electromagnetic noise, the resulting EMI (Electro Magnetic Interference) can interfere with the operation of the WLAN. The MAC sub layer of 802.11 is based on the CSMA/CA channel access method in which a station will first listen for an open channel before transmitting. This is done by sensing the energy level in the frequency band corresponding to the channel. In an environment with significant levels of EMI, the noise floor in the operating frequency ranges of 802.11 networks can prevent stations from transmitting because the RF energy threshold level for an open channel has been exceeded. Essentially, the WLAN stations believe that all of the channels are in use by other stations and hold off on transmissions. This can obviously create performance problems for WLAN networks operating in high EMI environments and should be taken into consideration.

   Possible mitigations include:

   a. Using the less susceptible frequency band (802.11a or 802.11b/g) for a given industrial environment.

   b. Configuring the stations and access points to use a particular fixed channel that is less affected by the EMI.

   c. Deploying directional antennas.

   d. Using a Frequency Hopping (FH) radio with configurable hopping channels and patterns.

   Note: A FH radio implementation can offer improved EMI immunity in an industrial environment as well as provide an additional measure of security if an unknown hopping pattern is used and also changed on a periodic basis. However, the Physical Layer will be proprietary in nature and not compatible with a WLAN station or access point based on one of the IEEE 802 a/b/g Physical Layer interoperable standard protocols. Additionally, the FH radio will have a reduced data rate relative to the existing standard 802.11 Physical Layers (typically less than 2Mbps). These factors and customer requirements should be taken into account when considering a FH radio implementation.

   In addition to EMI, Radio Frequency Interference (RFI) generated by transmitting WLAN stations and access points should be considered. The frequencies used may interfere with industrial control and monitoring equipment. The RFI may even

interfere with other wireless communication systems that may be deployed in the plant (e.g. 802.15.4 mesh networks using the 2.4GHz ISM spectrum).

Possible mitigations for RFI include:

a. Reduced transmission power levels.

b. Configuring the stations and access points to use a particular fixed channel that produces less interference.

c. Using directional antennas.

d. Placement of access points and stations.

e. Using a Frequency Hopping (FH) radio with configurable hopping channels and patterns.

2) *Reliability*: Consideration should be given to the types of applications that operate over WLAN networks deployed in industrial environments. RF transmission quality and reliability are affected by many factors in the operating environment, many of which are dynamic in nature. As mentioned above, EMI from factory or process machinery can cause degradation of WLAN performance, and objects in the path of the receiver can cause reflections resulting in attenuated multi-path reception issues. In factory environments with an abundance of machinery and metal objects that are both static and dynamic in nature (conveyors, cranes, robotic devices, etc.), reliable wireless communication may present a challenge. Therefore, the types of applications, their criticality, and the performance, reliability, security, and availability requirements should be analyzed and tested before deployment over WLAN networks.

   Note: The ISA-SPA100.14 Working Group has developed a set of *usage classes* that categorize inter-device industrial wireless communications based on such factors as importance of message delivery timeliness, the function of the application, and the type of system (safety, control, monitoring). This can serve as a useful starting point for assessing criticality.

3) *Security*: Related to the issue of reliability is security. This paper has discussed the security design principles and recommended practices for securing WLAN networks. By applying these principles and practices, the security risks of deploying and operating a WLAN network can be mitigated. As with any network implementation, security is only as effective as the controls implemented and the practices followed by those who use and manage it. However, with WLAN networks, because of the nature of RF propagation, the perimeter cannot be contained and controlled to the degree possible with a wired network. Signals will reflect off objects and find their way out of a building. Motivated attackers can attempt to detect these stray signals, however low-strength they may be, and attempt to interfere with the WLAN if they are in physical proximity of the facility. Attackers can passively capture traffic and attempt to penetrate the WLAN and the wired network to which it is attached. Attackers can

also attempt to more actively interfere using RF jamming denial-of-service (DOS) techniques that flood the frequency spectrum used by WLAN devices so that the channels become unavailable for transmission.

K. Conclusion

Strong Layer-2 security can now be used to protect WLAN networks based on the IEEE 802.11i standard. The original 802.11 WLAN security standard based on WEP had security flaws that made implementations vulnerable to weak key attacks. The interim WPA standard addressed the most pressing problems with WEP, and the 802.11i standard now provides a permanent, strong security replacement for WEP. 802.11i provides frame level encryption, authentication, and integrity protections for WLAN traffic. It also provides mutual authentication mechanisms based on the 802.1x protocol and Pre-Shared Key (PSK) methods. WLAN products that are tested and certified as being compliant with the 802.11i standard are known as "WPA2 compliant".

Customers considering deploying WLAN networks in their environments for non-critical industrial applications should consider adopting the 802.11i security standard for WLAN traffic protection, applying the secure WLAN design principles discussed in this paper during the planning phase, and implementing the recommended security measures outlined in this report during the deployment phase.

Industrial customers considering deploying WLAN networks in their environments for more critical applications should consider the issues of interference, reliability and security discussed in this paper as well as the security measures and threat mitigations presented. The degree of criticality, risk, and whether a given industrial application is appropriate for use over a WLAN network should take into account the material presented in this paper but is ultimately a determination that must be made by the organization responsible for its implementation and operation.

L. Online References

Below are online references related to WLAN technology and security.

1) The Wi-Fi Alliance:

   http://www.wi-fi.org

2) Comprehensive paper on Deploying WPA and WPA2 in the Enterprise:

   http://www.wi-fi.org/white_papers/whitepaper-022705-deployingwpawpa2enterprise/en

3) The IEEE 802.11 Working Group:

   http://www.ieee802.org/11

4) The ISA Working Group 100.14 is developing standards for industrial wireless and has developed a set of usage classes for various applications:

   http://www.isa.org

5) This site is a good resource for wireless security, information, tools, and vulnerabilities:

   http://www.wirelessdefence.org

6) An interesting step-by-step guide for cracking the WEP protocol:

   http://www.wirelessdefence.org/Contents/stepbystepWEP.htm