CHAPTER 33

802.11 WIRELESS LAN SECURITY

Gary L. Tagg, CISSP and
Jason Sinchak, CISSP

33.1 INTRODUCTION. IEEE 802.11 wireless local area networks (LANs) are now ubiquitous and have major benefits such as mobility, flexibility, rapid deployment, and cost reduction over traditional wired networks. However, as with any networking technology, wireless LANs create opportunities for unauthorized individuals to potentially access the enterprise network and the information carried over it.

This chapter provides an overview of wireless LAN technologies, security threats and attacks, and how to address them. It is structured as follows:

- 802.11 history and technological overview
- 802.11 security fundamentals
- Detailed coverage of 802.11 security covering both the original legacy functionality and the upgraded system first defined in 802.11i-2004
- Fundamental wireless-medium security threats
- Specific technical wireless-LAN security attacks
- Technical mitigating controls for specific security attacks
- Overarching secure enterprise design principals

33.1.1 Scope. The scope of this chapter is the security of ANSI/IEEE standard 802.11 wireless LANs. This chapter does not consider any other wireless systems, such as mobile telephone networks, or other wireless standards such as HomeRF, Bluetooth, WiMax, or HiperLAN. This chapter provides a high-level overview of fundamentals with technical deep dives in specific areas necessary to comprehend threats. Many of the basic terms and concepts are documented in Chapter 32 in this *Handbook*.

33.1.2 Corporate use of Wireless LANs. Corporations have been using wireless LANs since the 1990s. However, to begin with, the market was fairly small and the technologies proprietary. In the late 1990s and early 2000s, the groundwork was laid for the mass adoption of wireless LANs. The starting point was the publication of ANSI/IEEE standard 802.11 that provided a baseline design enabling manufacturers to develop interoperable products at lower costs.[1]

33.1.3 Functional Benefits of Wireless. The main advantages of implementing wireless networks are mobility, flexibility, and cost reduction.

- **Mobility:** Wireless technologies enable staff to access network information via mobile terminals as they move around the office campus; examples include warehouses, shop floors, and hospitals. Within an office environment, wireless technologies provide a flexible alternative or addition to the wired network. Often, desks and meeting rooms have a limited number of Ethernet connections; wireless technologies can cost effectively provide additional network connections as required.
- **Flexibility:** Public wireless networks (hotspots) allow staff to utilize idle time between meetings, in airports, coffee shops, and even on airplanes in flight.[2] Typical uses include access to the corporate LAN, along with information on the Internet. Public hotspots can also be trunked over the enterprise wireless LAN to provide internet access for consultants and visitors.
- **Cost Reductions:** Costs can be lowered by not having to install physical network links between buildings separated by a road, river, railway tracks, or even a city block. A wireless link can be set up between two buildings provided there is an uninterrupted line of sight between them. In addition, economies of scale can be realized with a wireless medium. A single access point (AP) (thick or thin) can service one or many end users and scale appropriately by bumping excessive users to neighboring APs. This capability is exclusive to wireless. A wired network has a fixed capacity for per-port access and virtual LAN (VLAN) assignment. The use of wireless with Service Set Identifier (SSID) VLAN support can reduce the networking hardware volume. In the case of dynamic VLAN assignment within a wired LAN, endpoint or server moves require proper VLAN pruning at the switch layer to retain security yet provide the required VLANs. Cost savings can be realized within a wireless LAN by reducing network-management tasks and overall complexity to maximize resources and hardware usage.

33.1.4 Security Benefits of Wireless

- **Physical Security:** An AP and supporting hardware can be hidden from end users to protect it from physical attack. A wireless AP can be hidden above the ceiling in contrast to physical endpoint network jacks, which must be accessible by all users who need access to the internal network. This leaves the door open for unauthorized access to a network port in the absence of enterprise wide 802.1X port security.
- **Segmentation Visibility:** Wired networks commonly assign VLANs on a per-port basis, or in advanced configurations, using one per Media Access Control (MAC) address. In port-based VLAN assignment, management relies heavily on proper access-layer switch configuration and the pruning of sensitive VLANs not necessary for a specific business unit or location. MAC address-based VLAN assignment requires the use of MAC authentication-aware switch hardware and a backend authentication and RADIUS server for MAC → VLAN mappings. MAC-based VLAN assignments can improve management capability and oversight, but pose a significant security risk as they are susceptible to MAC-address spoofing.

In a wireless environment, VLANs can be assigned on a per-SSID basis and administrative efforts can be greatly reduced. A user is no longer confined to a particular

physical location for access to a necessary VLAN, as long as the SSID is available on accessible APs. In the event of expansion, deploying a new AP in close proximately will deliver the necessary VLANs with the corresponding SSID that a client supplicant profile is configured to search for. Since VLAN assignment can be controlled through minor client supplicant configurations and backend RADIUS privileges, segmentation can be determined during the asset-provisioning process and require relatively minor management thereafter.

In an environment which relies heavily on access-layer switches for endpoint connectivity, it is not uncommon to find switching or upstream router protocols making their way to access-layer switch ports. These include protocols such as Dynamic Trunking Protocol (DTP), VLAN Trunking Protocol (VTP), Hot Standby Router Protocol (HSRP), Cisco Discovery Protocol (CDP), Open Shortest Path First (OSPF) routing, and so on. A user with port access can exploit multiple known vulnerabilities in these protocols.

33.1.5 Centralized Management. Thin-client AP environments leverage wireless controllers to provide a central configuration for all associated APs. Thin-client APs are configured on the controller, and intelligence is provided by a backend user directory (Extensible Authentication Protocol–Remote Authentication Dial In User Service, or EAP-RADIUS) and controller itself. The widespread yet central connection of a mesh of APs can additionally be leveraged for security monitoring of the wireless airwaves in a Wireless IDS fashion as described in Section 33.4.

33.1.6 Overview and History of the IEEE 802.11 Standards. The first IEEE 802.11 standard was published in 1999. Following publication, work continued on developing 802.11 with amendments published on a regular basis. The publication of the 802.11b standard increased WLAN bandwidth from 2Mb/s to 11Mb/s, making it a possible technical replacement for a wired LAN. Following that were the 802.11a and 802.11g standards that increased throughput further to 54Mb/s.

These and other amendments were then brought together in the revised standard 802.11-2007. Development continued via further amendments, which were once again brought together with the issue of 802.11-2012.[3]

The first version of the standard contained authentication and confidentiality services in an attempt to provide similar levels of security as wired LANs. The authentication service consisted of two systems called *Open Authentication and Shared Key Authentication*, and the data confidentiality service was called *Wired Equivalent Privacy* (WEP). These services are often referred to as the *legacy security services*.

In 2004 the 802.11i standard was released and defined the *Robust Security Network* (RSN) system, which provided enhanced authentication and confidentiality services. The authentication service has two options: the first is the use of pre-shared keys targeted for homes and Small Office Home Office (SOHO) users and the second uses the 802.1X/EAP framework for enterprise use.

Following the issue of the 802.11-2007, amendments were introduced to provide security mechanisms for mesh wireless networks and the use of 802.11 for transportation applications. There were also enhancements to the core 802.11i algorithms to secure some management frames, and enable fast transition to other APs for time critical services such as Voice over IP (VoIP). Throughput was further improved to a maximum of 600Mb/s by the release of 802.11n-2009.

Exhibit 33.1 provides an overview of the development of the 802.11 standard, the amendments, and identifies those with security functionality using shading.

33.2 802.11 SECURITY FUNDAMENTALS. This section describes the underlying 802.11 security fundamentals in preparation for the details covered in later sections.

33.2.1 Terminology. To better understanding this chapter, readers will find clarification of a few commonly misunderstood 802.11 terms. Section 0 has a more extensive glossary.[4]

Authentication: Authentication is the first step in a two-step process of client connection to an AP. This step validates the client's authority to start associating

with the AP. Network-based authentication such as username and password takes place after layer 2 authentication and association.

Association: Association is the process of the AP accepting the client connection and allocating resources for it. This includes things such as adding client specific information such as supported data rate, data protocol 802.11 b/g/n, and MAC address information.

802.1X: 802.1X provides the encapsulation of Extensible Authentication Protocol (EAP) implementations within 802 communication mediums. 802.1X does not define a specific authentication method, but provides a vehicle for EAP implementations and their underlying methods. 802.1X and ultimately 802.11i are major components of the modern 802.11 RSN system. 802.1X allows or denies client access to requested resources until the client is successfully authenticated.

RADIUS: *Remote Authentication Dial In User Service* (RADIUS) is a network protocol used for authentication, authorization, and accounting (AAA). Historically, RADIUS servers leveraged a flat-file directory for user-based access decisions, but modern implementations leverage a dedicated directory such as Windows Active Directory, Lightweight Directory Access Protocol (LDAP), or a rational database such as Microsoft SQL Server or Oracle. In a Robust Security Network (RSN), a RADIUS server is only responsible for brokering the authentication/authorization of a user requesting access to an AP. Authentication data is transparently sent from the client to the RADIUS server by the AP, and the RADIUS server leverages an external directory to determine a response.

SSID versus BSSID: An SSID is a unique identifier used by a client to establish connectivity to a particular wireless network. An AP can provide multiple SSIDs on the same channel through the use of the same or multiple interfaces. A BSSID is the unique identifier for a Basic Service Set (BSS). A BSS consists of an AP and associated clients or clients.

An **Extended Service Set** (ESS) is a series of BSSIDs (AP interfaces) sharing the same SSID. This helps enable a wireless client to seamlessly move between APs using the same SSID. A BSSID is a separate interface with its own MAC address; multiple SSIDs can share the same interface and MAC address. On a commercial AP the first SSID/VLAN pair will use the BSSID interface/MAC address and each SSID after that will use a virtual MAC address, which increments the BSSID by a small value for each SSID. A BSSID can be used to reference a unique interface or AP (assuming the AP only has one interface). Depending on the vendor of a particular AP, a single BSSID will send broadcast beacons with all SSIDs in one sweep. If an SSID is placed on its own BSSID, it will have a dedicated beacon, which may improve compatibility.

33.2.2 Authentication and Access Control. In the absence of 802.1X port security, wired-LAN access control is primarily reliant on physical security. To access the LAN, an attacker first needs to have physical access to a connection point. In contrast, the nature of wireless LANs means any wireless client within radio range can potentially connect to the internal LAN network, bypassing physical controls.

To address this issue 802.11 provides an optional native-authentication service. The legacy 802.11 standard includes two protocols, open authentication and shared key authentication. Neither of these protocols was adequate for secure access.

Open authentication is a null-authentication service allowing any and all clients to connect and associate. Shared key authentication (SKA) requires the client to use a cryptographic key to successfully authenticate. This method did put a lock of sorts on the network, but it was soon exploited by attackers who acquired keying material to help compromise the system.[5] SKA lacked unique authenticated user tracking, and forced an out-of-band key management process. SKA has since been deprecated and should not be used, except for necessary backwards compatibility with older devices. The legacy 802.11 security system did not provide any access-control functionality. Although most equipment included access filtering based upon MAC address, this control was not part of the standard and the legacy service is therefore easily defeated.

The RSN defined by 802.11i is a much stronger system, and provides multiple mechanisms to authenticate the device and the user.[6] The system defines a personal profile for home/SOHO use based on PSKs, as well as an enterprise profile based upon the 802.1X/EAP framework, which allows the use of a backend authentication server. The 802.1X authentication system also allows for access control decisions to be taken by the network to restrict network resources available to an authenticated user through technologies such as VLAN segmentation.

33.2.3 Data Confidentiality. Data confidentiality on a wired network is provided by physical security and layer-2 boundaries, which limit the accessibility of the data. Unless an attacker is physically connected to the wired LAN and logically resides between a sender and recipient on the network, through ARP poisoning or physical position, the data traveling over the network cannot be captured. A wireless LAN uses a physically public medium for data transfer; therefore, every packet traveling between a wireless client and an AP is transmitted via radio signals and can be captured by any client within radio range. Although captured data may be encrypted and not readily viewable, it should be noted that any client can obtain the ciphertext in some manner despite layer-2 or logical boundaries.

To address this issue the 802.11 standard provides a data confidentiality service. The legacy system provided the Wired Equivalent Privacy (WEP) protocol, which encrypted each message with a symmetric key before transmission. However, this protocol was successfully attacked and automated tools built to enable WEP keys to be cracked by anyone with basic IT skills and access to the freely available toolset.[7] Overtime, improvements have been made to the WEP protocol, moving it toward a more respectable enterprise solution, but these fell short and were soon superseded by newer, ground-up protocols. Additional controls are needed to protect the network if WEP must be used, such as with older existing equipment.

The RSN system provides two new data confidential protocols called *Temporal Key Integrity Protocol* (TKIP)[8] and *Counter Mode with Cipher-Block Chaining Message Authentication Code Protocol* (CCMP).[9] As well as confidentiality, both protocols provide message integrity as well.

33.2.4 Key Management. Secret-key encryption itself is a relatively simple process designed to protect data long enough for the encryption keys to be changed at a determined interval. Designers start by choosing a suitable proven algorithm, protocol, and key length that they are confident will protect user data for a defined

period. The user (or user program) then provides that algorithm with the plaintext data and an encryption key, and the data are then encrypted and ready for transmission. Due to the rapidly advancing speed of processing (of individual CPUs and CPUs running in parallel), no level of any encryption can provide definitive protection for an unlimited period of time—the time required for brute-force testing of all possible keys in the keyspace—necessitating the need for a key scheduling and management system.

Securely and repeatedly establishing mutual encryption keys is the single most complex issue plaguing cryptographic communications between two parties in physically separate locations. The repeatable process of creating keys, mutually (and securely) exchanging different keys or independently deriving the same key, and finally destroying them, is key management.

The legacy 802.11 algorithms did not provide any specific key-management functionality and vendors were left to design their own. The most common system in early standalone APs was to manually enter a defined-length static WEP key into each client and AP. For home users, the RSN system defines the manual entry of a common variable length PSK or passphrase in the client and AP. From this PSK, a key-management process derives working cryptographic keys, which are changed for each message.

For enterprises, RSN uses the 802.1/EAP framework to establish a secure channel during the user- and device-authentication phase, allowing a pairwise master key (PMK) to be set up between the client and the AP. From this PMK, a key-management system establishes working cryptographic keys which are changed for each message.

33.3 IEEE 802.11 ROBUST SECURITY NETWORK.

In June 2004, the IEEE released the 802.11i standard to improve the security of 802.11 networks. This new system is called the *Robust Security Network* (RSN) and is designed for both personal and enterprise users. Enterprise use is based on the 802.1X protocol to provide authentication and establish a security context. A "personal" profile uses a *pre-shared key* (PSK) based on a password provided for consumers and SOHO users who do not require the necessary 802.1X backend authentication infrastructure.

33.3.1 Features.

The core protocol of RSN is IEEE 802.1X, which forms *RSN Associations* (RSNA) with the wireless network. RSN provides the following features:

- Mutual authentication mechanisms. These mechanisms can authenticate users as well as the network client or machine. The AP and backend authentication server can also be authenticated to the client defeating rogue AP and man-in-the-middle attacks.
- Key-management algorithms
- Cryptographic key establishment (through PMK and Pairwise Transient Key [PTK] establishment)
- Cryptographic message integrity codes to defeat the bit-flipping attacks possible in the original standard (WEP)
- Two data privacy protocols which also implement message integrity:
  1. *Temporal Key Integrity Protocol* (TKIP), which is an optional protocol specifically designed so that existing WEP based hardware can be upgraded to use it.

2. *Counter Mode with CBC-MAC Protocol* (CCMP), which is mandatory for RSNA compliance. It uses the Advanced Encryption Standard (AES) in Counter mode for confidentiality and CBC-MAC for authentication and integrity. CCMP is a strong protocol that has been designed for the next generation of wireless equipment.

TKIP was designed as a temporary stopgap that would work on existing WEP-based hardware until new hardware containing the CCMP protocol became commonplace. Whereas TKIP continued to use the existing RC4 encryption algorithm that was at the heart of WEP, CCMP uses the AES algorithm and requires more powerful hardware—no longer a problem at present.

33.3.2 802.1X Overview. 802.1X was originally designed for port-based network-access controls for IEEE 802 LAN infrastructures. These infrastructures include Ethernet, token ring, and wireless networks. 802.1X authenticates and authorizes devices attached to an LAN port, and will not allow a device to access the network if authentication fails.

802.1X defines three roles:

1. **Authenticator**. The device that authenticates a network device before allowing it to access network resources. In an 802.11 BSS network the AP is the authenticator.
2. **Supplicant**. The device that wants to access network resources and needs to be authenticated.
3. **Authentication Server (AS)**. The AS performs the actual authentication of the supplicant on behalf of the authenticator. The AS can be located with the authenticator, but is commonly an external system such as a RADIUS server.

The 802.1X standard defines the object *Port Access Entity* (PAE) which operates the authentication algorithms and protocols in the supplicant and authenticator. An overview of the 802.1X architecture is shown in Exhibit 33.2 below.[10]

The authenticator has two logical ports; the first is an uncontrolled port that allows access to required functionality such as the authenticator PAE. The second port is the controlled port that allows access to the rest of the network. The status of the controlled port is set by the authenticator PAE and is dependent upon the outcome of the authentication between the supplicant and the authentication server.

The messages between the supplicant and authenticator use the Extensible Authentication Protocol (EAP) over LAN (EAPoL) framework defined in 802.1X. Communications between the authenticator and the AS leverage the EAP framework carried in a higher-layer protocol such as RADIUS.

33.3.3 EAP, EAPoL, and PEAP. 802.1X relies on EAP[11] to perform authentication of the supplicant and authenticator. The EAP protocol is a series of method interfaces that make up the framework known as EAP. EAP was originally designed for use on modem dial-up networks; therefore, the 802.1X specification details the expansion of EAP across Ethernet/Token Ring networks through the EAPoL (EAP Over LAN)[12] extension. In addition to placing EAP methods within an Ethernet payload, EAPoL specifies a number of additional functions to assist in the authentication process during discovery and key exchange. There are currently over 40+ different implementations of the EAP framework. The primary difference in EAP implementations centers on how the supplicant and authenticator are authenticated.

Standard EAP is not a mutual authentication protocol; only the supplicant is authenticated. This makes supplicants vulnerable to rogue AP attacks. Additionally, due to its original design for physical dial-up connections, EAP does not protect its authentication messages from eavesdropping. Therefore, the current EAP/EAPoL implementations establish secure tunnels to provide security prior to exchanging authenticating material. The following are the most common EAP/EAPoL enterprise 802.1X implementations ranked by the level of afforded security:

1. **EAP-TLS**[13]**:** This EAP implementation only allows mutual certificated-based authentication through *Transport Layer Security* (TLS) X509 certificates. Authentication of both the backend authenticating server and wireless client provides a strong level of wireless security, but requires a full enterprise *Public Key Infrastructure* (PKI) implementation to securely distribute and update client keys on a regular basis. An issue with EAP-TLS is most organizations do not have the necessary PKI to issue the supplicant client TLS certificates.
   - **EAP-TTLS** (*Tunneled TLS*)[14]**:** EAP-TTLS is similar to EAP-TLS and supports mutual certificate authentication but does not require client-side certificates. EAP-TTLS creates a TLS tunnel prior to starting any network authentication process and can therefore tunnel any password authentication mechanism, even insecure legacy mechanisms such as PAP.
2. **EAP-PEAP** (*Protected EAP*)[15]**:** In its native form, EAP-PEAP does not support mutual certificate-based authentication. Native EAP-PEAP uses TLS to authenticate the backend directory server only and leverages a password-based challenge-response process to authenticate the client. Later PEAP extensions help to mitigate this weakness. EAP-PEAP is native to most Microsoft Windows versions and is therefore very prevalent across the wireless industry. There are currently three primary types of EAP-PEAP, which provide varying levels of protection:
   - EAP-PEAP-MS-CHAP-v2 (*Microsoft Challenge Handshake Authentication Protocol*)[16]**:** The most common EAP-PEAP inner authentication method uses Microsoft's CHAP-v2 protocol to provide user-identifier (userID) and password challenge–response-based authentication. The MS-CHAP authentication process has historically allowed an attacker with physical access to the AP, to capture the provided challenge and challenge-response hash in plaintext. Due to recent cracking advancements, the time to crack an

MS-CHAP-v2 challenge-response hash has been reduced to days or less and should be avoided at all costs unless proper client supplicant configurations can be established.[17] This process is described in section 0 of this chapter.

- EAP-PEAP-TLS[18]**:** PEAP-TLS is the second PEAP inner protocol defined by Microsoft. PEAP-TLS tunnels the EAP-TLS protocol within PEAP to provide mutual X509 certificate-based authentication.
- EAP-PEAPv1 (EAP-GTC): The third implementation is defined by Cisco, which allows authentication using generic token cards such as RSA's SecurID token as well as user ID and password.

3. **EAP-LEAP**[19]**:** A proprietary protocol developed by Cisco, which performed challenge-response MS-CHAP-v2, based username/password authentication in cleartext. An attacker targeting a network employing EAP-LEAP only needs to monitor traffic to capture challenge-response hashes for offline dictionary attack. This is in contrast to EAP-PEAP-MS-CHAP-v2, which requires a rogue masquerading AP for an attacker to intercept MS-CHAP-v2 challenge-response hashes.
4. **EAP-FAST**[20]**:** (Flexible Authentication via Secure Tunneling) was developed by Cisco as a replacement to the vulnerable LEAP protocol. EAP-FAST introduced secure pre-authentication tunnels without using certificates. EAP-FAST has secure mutual authentication capabilities, but also has an automatic PAC provisioning option—which is vulnerable to man-in-the-middle attacks.

33.3.4 Insecure Legacy EAP protocols. When EAP was first integrated into 802.11, the EAP-MD5 and Cisco's EAP-LEAP protocols were commonly used. Unfortunately, these turned out to be vulnerable to attack, which spurred the development of the secure protocols covered above. EAP-MD5 and EAP-LEAP should not be used for enterprise wireless deployment.

33.3.5 Detailed EAP/EAPoL Procedure. Exhibit 33.3 shows the high-level RSN security association management flow. It consists of five stages that:

1. Establish a secure channel between the authenticator and authentication server
2. Locate the network, negotiate cryptographic algorithms, and associate to it
3. Provide 802.1X authentication to the authentication server
4. Provide Mutual Authentication and establish pairwise cryptographic keys
5. Establish Group/Multicast cryptographic keys

The following sections describe these stages. There are two aspects that vary the security association flow. The first is whether the wireless network contains an Access Point (a *Basic Service Set* or BSS) or whether it is an *independent* BSS (IBSS), also known as an *ad-hoc network*, which is a peer-to-peer network topology.[21] The second is whether the master cryptographic key is a global PSK or if it is established during the 802.1X authentication protocol. Any variations caused by BSS/IBSS and 802.1X/PSK are described within the sections.

Stage 1—Establish a Secure Channel between Authenticator and Authentication Server