Global Information Assurance Certification Paper

802.11 Wireless Security vs. Basic Network Security Principles

Tom Hollingshead

GSEC Practical Assignment, ver 1.4b - Option 1

22 December 2003

Abstract

An IEEE 802.11 standard wireless network is easily installed, flexible, inexpensive to deploy and very functional in that speeds of up to 54mbs are now possible. While the ease and cost to deploy are attractive selling points, the inherent security risks associated with wireless networking are a major factor to take into consideration before implementing a wireless LAN on any network, especially those with critical or sensitive resources available from it.

My goal in this paper is to present the basic security issues associated with an 802.11 wireless local area network(WLAN) and the IEEE based options available to remedy them. There are many specifications included in the 802.11 standard architecture. I will be focusing on the aspects of the 802.11 architecture that apply to the network security principles of Identity, Authentication and Authorization and how they in turn affect the Confidentiality, Integrity and Availability of the associated network resources. I will begin by describing the basics of the 802.11 standard's architecture to show how well it applies basic network security concepts. And to point out the inherent vulnerabilities to use as a foundation to better understand the options available to secure an 801.11 network. I will then cover the IEEE based options available to strengthen 802.11 wireless networks such as 802.1x, Wi-Fi Protected Access (WPA) and 802.11i. I will finish up by comparing the security weaknesses present in the original 802.11 standard to how 802.1x, WPA and 801.11i are used to strengthen 802.11 wireless networking.

Wireless Basics

Definitions

"The IEEE 802.11 standard is defined as Wireless LAN Media Access Control(MAC) and Physical Layer(PHY) specifications."[1]

"Station (STA): Any device that contains an IEEE 802.11 conformant medium access control (MAC) and physical layer (PHY) interface to the wireless medium(WM)."[1] This is basically a network node that has a wireless network device installed that can send and receive wireless transmissions.

"Access Point (AP): Any entity that has station functionality and provides access to the distribution services, via the wireless medium (WM) for associated stations."[1] An AP is a network node that has the same ability to send and receive wireless transmissions as a

[1] ANSI/IEEE Std 802.11, 1999 Edition

STA and also has an interface that allows it to communicate with a wired network and in this way functions as a bridge between wireless networks and wired networks.

Service Set Identifier – SSID: "The SSID identifies a specific wireless LAN. Before associating with a particular wireless LAN, a station must have the same SSID as the access point."[2]

"Basic Service Set – (BSS): A set of stations controlled by a single coordination function."[1] This is the most basic component of an 802.11 WLAN. Can be classified as either an Independent BSS (IBSS) or an Extended Service Set (ESS). An ESS is a single logical network and is identified by SSID.

"Distribution System - (DS): A system used to interconnect a set of basic service sets (BSSs) and integrated local area networks (LANs) to create an extended service set (ESS)."[1]

Modes of Operation

The IEEE 802.11 standard specifies two operating modes: Ad hoc mode and Infrastructure mode.

Ad hoc mode is basically directly connected peer-to-peer networking. Each station's WLAN adapter is configured for Ad hoc mode with identical settings and will then be able to connect directly to the other station without the use of an AP as long as they are within range of the other station. See figure 1 below for an example of an Ad Hoc WLAN.

Figure 1 – Ad hoc wireless network

Two or more wireless clients who communicate using ad hoc mode form an Independent Basic Service Set (IBSS).

An Infrastructure WLAN is made up of wireless stations and access points and takes advantage of the added functionality that access points provide. An AP not only acts as a bridge between the wired and wireless networks it also serves to control wireless network traffic within its wireless coverage area. An AP can also make use of the

[1] ANSI/IEEE Std 802.11, 1999 Edition
[2] www.wi-fiplanet.com – tutorial 1492071

distribution system(DS) which allows multiple BSSs to be combined to form an extended service set(ESS) thus extending the WLAN's area of coverage and allows greater mobility for roaming stations. The added functionality of Infrastructure WLAN makes it more flexible and scalable than the simple peer-to-peer Ad Hoc WLAN and consequently the vast majority of WLANs in use today operate in Infrastructure mode. See figure 2 below for an example of a simple Infrastructure mode WLAN.

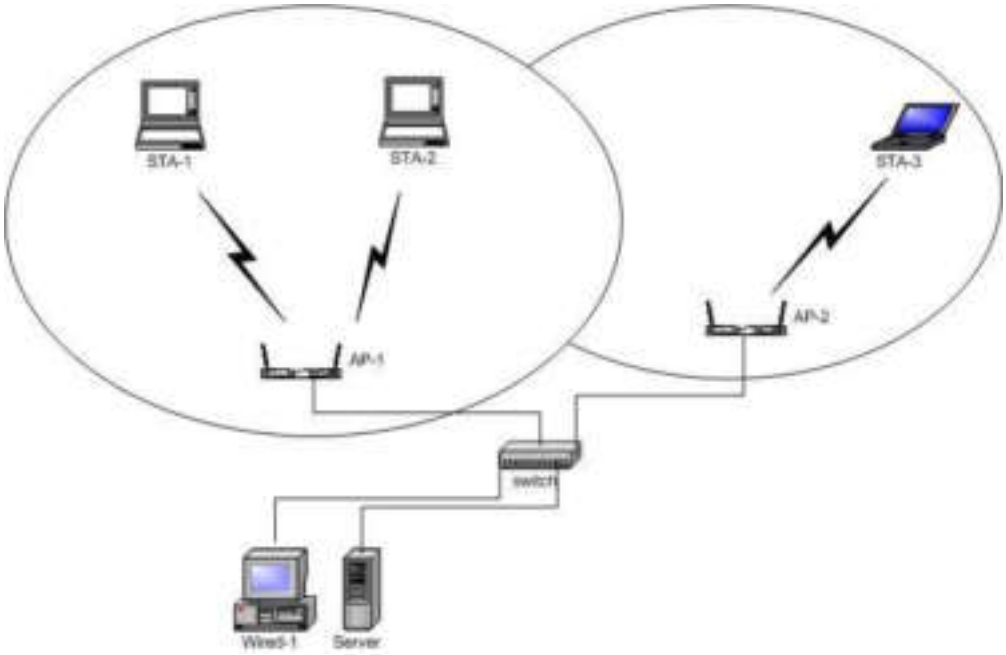

Figure 2 – Basic Infrastructure Mode WLAN

WLAN Security or Lack Thereof

Any discussion of network security should cover the basics principles of identity, authentication, and authorization as they apply to the network being discussed. While the IEEE 802.11 standard does specify two forms of authentication to be used when connecting to an 802.11 WLAN, the identity and authorization portions of network security are either scant or missing entirely. Even the two authentication methods that are specified have some major issues in relation to real network security. The two methods of 802.11 authentication are open authentication and shared key authentication.

Open authentication is really no authentication at all. The only requirement to authenticate with open authentication is to provide the SSID of the STA(in Ad Hoc mode) or AP that the STA is attempting to connect to. By default most access points are configured to broadcast the SSID on the airwaves so the STA will automatically know the SSID and be able to connect to the AP with virtually no authentication. Open authentication will be covered in more depth in a later section.

Shared key authentication, while better than the virtually nonexistent authentication of open authentication, has some major problems also. The problems with shared key authentication are twofold. One, it is based on the WEP algorithm. WEP at its core is flawed because it uses a 24-bit key as the Initialization Vector for part of the authentication scheme. By current cryptographic standards a 24-bit key is very weak. WEP also uses the same key for all operations, for all hosts. Two, the lack of any key management procedures to automatically determine and distribute keys used for shared key authentication. The problems with WEP and Shared Key authentication will described in more detail in another section.

Wireless Connection Protocol

In order to better understand wireless network security issues it is helpful to be familiar with the various wireless connection processes that apply to network security. This section will cover the common wireless communication process between a wireless station(STA) and an access point(AP). There are three phases in the communication process in relation to a wireless STA connecting to an AP; network discovery/selection, authentication/association, and disassociation/reassociation. The primary focus in this paper will be on the first two phases as that is where the majority of the security related issues are found. Figure 3 below shows the steps in a typical wireless connection:

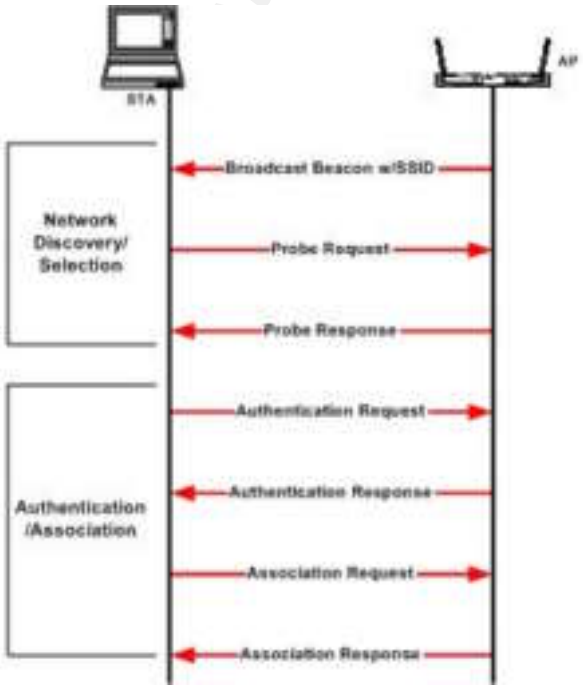

Figure 3 – Basic Wireless Connection

Since the AP plays a critical role in all aspects of the wireless communication process describing how an AP works is a good place to start. An AP broadcasts what are called

beacon frames. A Wi-Fiplanet.com tutorial describes the function of beacon frames like this:

> The access point periodically sends a beacon frame to announce its presence and relay information, such as timestamp, SSID, and other parameters regarding the access point to radio NICs that are within range. The radio NIC in a STA continually scans all 802.11 radio channels and listen to beacons as the basis for choosing which access point is best to associate with.[3]

An AP's beacon frames play a vital role in the wireless connection process. "The beacon frame, which is a type of management frame, provides the "heartbeat" of a wireless LAN, enabling stations to establish and maintain communications in an orderly fashion."[2] A wireless STA must obtain the SSID of the AP that it is attempting to connect to or associate with. By default APs include the SSID in the beacon frame to facilitate automatic configuration and connection of the wireless STA.

Discovery/Selection

To start the connection process the STA will begin to try to discover a network to connect to and is by default doing passive scanning. As mentioned above, the STA is scanning each channel listening for beacons so that it can gather the necessary information to determine the most optimum AP to connect to. Also available for the STA is active scanning. "Active scanning is similar, except the STA initiates the process by broadcasting a probe request frame, and all access points within range respond with a probe response. Active scanning enables a radio NIC to receive immediate response from access points, without waiting for a beacon transmission."[4] "The STA uses the beacons or probe responses to determine which AP is the best AP for selection for the next phase in the connection process."[2]

Authentication

Once the STA has selected the best AP it starts the authentication process. The method of authentication, either Open or Shared Key, is determined by the AP and the STA will initiate authentication accordingly. Both methods will be covered next.

With Open authentication the STA simply sends an authentication request frame that contains it's MAC address as the source identity. The AP then responds back with an authentication response of accept or reject. By default there is no criteria to reject the STA's authentication request and so there is really no true authentication taking place, just a MAC address for identification. Many APs have an option to configure a MAC filter where only the MAC addresses added to the AP's MAC filter list are allowed to connect, in this case there a minimal level of authentication taking place.

---

[2] www.wi-fiplanet.com – tutorial 1492071
[3] www.wi-fiplanet.com – tutorial 1447501
[4] www.wi-fiplanet.com – tutorial 1216351

Shared Key authentication starts off with the STA sending an authentication request frame, the AP then responds with an authentication response frame that contains challenge text. The STA then encrypts the challenge text with it's WEP key and includes the results in another authentication frame to the AP. The AP decrypts the results it received from the STA and verifies whether it matches the original challenge text it sent previously and thereby verifying that the STA has the correct WEP/Shared Key. Based on the results of the challenge text comparison the AP sends back an authentication response frame either accepting or rejecting the authentication attempt. The STA has now been authenticated and continues to the next step. See figure 4, which includes the addition of the shared key authentication frames.

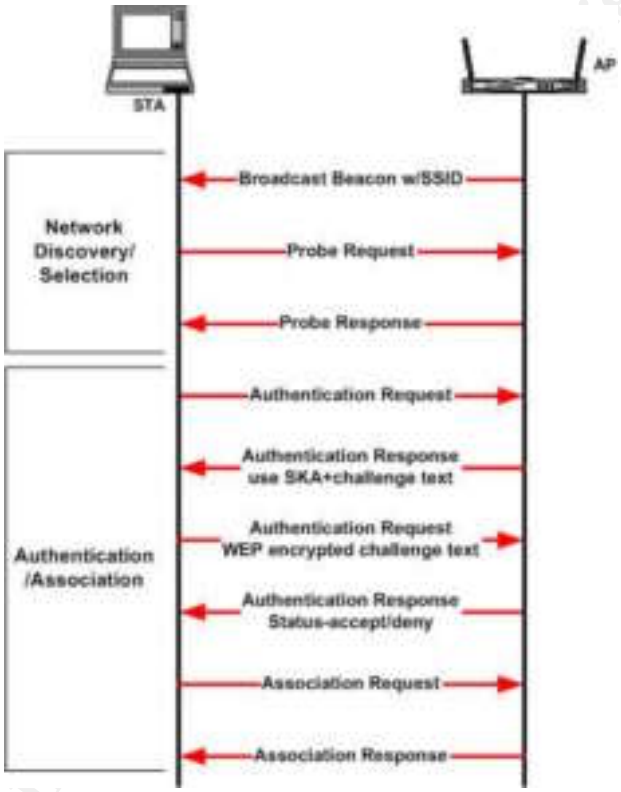

Figure 4 – Wireless connection with Shared Key Authentication

Association

The STA starts the association process by sending the AP an association request frame with, among other types of information, the SSID of the network it is attempting to associate with. The AP will then determine whether to accept or reject the request. Once the AP receives and accepts the request from the STA it "reserves memory space and establishes an association ID for the STA."[3] The AP then sends an association response frame that contains an acceptance or rejection notice. If it is an acceptance notice it will also include the association ID. "The STA is now associated with the AP and can use the AP to communicate with other STAs on the network and systems on the distribution side of the AP."[3]

[3] www.wi-fiplanet.com – tutorial 1447501

Disassociation - Reassociation
If signal strength from the AP becomes too weak or noisy the STA will start scanning for other APs with a better signal quality. If an AP with a stronger signal is found the STA will negotiate with the new AP to reassociate with it and disassociate with the old AP. This is how a laptop user roams between various APs and is able to maintain network connectivity while doing so.

802.11 Security Issues

Now that the basic 802.11 connection process has been explained we can take a closer look at what kind of effect those processes have on network security. This section will cover the various security issues related to 802.11 wireless networking.

Physical Issues
The very same aspects of wireless networks that make them so attractive like wide-open easy access and ease of implementation are also major problem areas for network security.

With a wired network users have to at least be able to plug into a physical LAN port in order to access network resources. There is no such restriction with a WLAN. If a radio NIC is in range of the AP it can connect and access the network. And since the range of the AP can extend beyond the boundaries of the office building, unauthorized access to user credentials and data that are being transmitted over the airwaves can be had without ever entering the premises. This aspect of a WLAN opens the door to session hijacking and loss of confidentiality of the data being transmitted. Not only is it a wide open door to session hijacking and eavesdropping problems it also makes it vulnerable to denial of service attacks where an attacker floods the airwaves with messages to the point that it causes availability problems.

The ease of implementation aspect also brings up issues with rogue APs being installed. An unauthorized, improperly configured AP installed on a corporate LAN can open a huge hole in the wired network. Or a hacker could setup an AP masquerading as a valid WLAN AP to lure valid users into using a bogus network while the attacker captures user credentials, etc.

Network Discovery/Detection Issues
By default most APs are configured so that ease in connecting is the priority over network security. Consequently, out of the box, APs are very easy to connect to but very insecure.

One of the AP's main functions is to transmit beacon frames in periodic broadcasts to advertise the AP's capabilities, synchronize wireless communications and announce it's presence on the network. By default the beacon frames will include the SSID of the AP.

Since the SSID in a basic sense is the equivalent to the password for associating to the network, broadcasting the SSID on the airwaves is a bad thing for network security.

It is possible to disable the broadcasting of the SSID in the beacon frames. When the SSID is not provided in the beacons the STAs attempting to associate with the AP must obtain the SSID by other means. In most cases the SSID will be provided when the administrator properly configures the STA. Other options that an attacker could use would be to guess what the SSID is or use a script using the default SSIDs that the various AP vendors configure in their APs out of the box. This could work if the default SSID was never changed. (You can check this link to see the default settings on most AP devices - http://www.cirt.net/cgi-bin/ssids.pl[5]) This is not a likely scenario since if the administrator took the time to disable SSID broadcasting they most likely changed the default SSID value also. The more likely option is that a slightly determined attacker could use is an application like Kismet[6] to sniff the wireless transmissions and pick up the SSID from authorized network traffic.

Authentication Issues

As stated before the two 802.11 authentication methods have some major problems for serious network security. This section looks at the problems in more depth to point out exactly what the problems are to get a better understanding of what needs to be done to resolve them.

Open Authentication – The problems with Open Authentication have been mentioned in previous sections. They include the fact that it is virtually no authentication at all. If the AP is broadcasting the SSID a STA will connect using just it's MAC and the AP has no criteria to reject the authentication request so all requests are accepted. A MAC filter configured on the AP would provide a minimal level of authentication in that it would at least give the AP some criteria to reject an authentication request. While MAC filters do add a level of security it is minimal since the STA's MAC can be spoofed using a MAC configurable radio NIC. Also MAC filtering does not scale to large networks as the MAC filter has to be manually configured on each AP.

Another issue with operating a WLAN using Open Authentication is that all radio transmissions are broadcast in clear text. No encryption of data is taking place and eavesdropping and packet sniffing would be very easy.

Shared Key Authentication – Shared Key Authentication is meant to provide a higher level of authentication than the virtually wide-open authentication scheme in Open Authentication. Shared Key Authentication does constitute an improvement over Open Authentication but in terms of being able to prevent a serious hacker from eavesdropping, gathering valuable information and gaining network access it is still lacking and has several major weaknesses. One problem is that Shared Key Authentication is based on the weak Wired Equivalent Privacy(WEP) algorithm. Another

[5] www.cirt.net/cgi-bin/ssids.pl
[6] www.kismetwireless.net

problem is the lack of any key management procedures to generate and distribute keys used for Shared Key Authentication.

Wired Equivalent Privacy – The WEP privacy mechanism used with Shared Key Authentication is easy to crack due to two factors.

As part of the authentication process, an AP responds to an authentication request from a STA with an authentication response that includes a challenge text for the STA to encrypt into ciphertext. This challenge text or WEP initialization vector(IV) is a pseudo-random key sequence[1] and is only 24 bits long which provides a range of only 16,777,216 possible different values. This is a relatively small key value in terms of cryptographic strength. With such a small key length it is only a matter of time, depending on the amount of network traffic, before the IV is reused. Given the fact that all wireless transmissions from both the AP and the STAs use the same WEP key for all communications including heavy data traffic, within a reasonably short period of time an attacker can easily capture enough of the packets where the IV has been duplicated or reused. They can then analyze the captured packets to determine the WEP key.

Another factor is that during the authentication process the challenge text(IV) from the AP's 1st authentication response frame is sent in the clear over the WLAN to the requesting STA. The encrypted ciphertext(WEP encrypted challenge text) from the STA's 2nd authentication request is also available on the WLAN. "An attacker can obtain both the challenge text and the ciphertext response and can derive the stream cipher by analyzing both the plaintext challenge and the ciphertext. This information can be used to build decryption dictionaries for that particular WEP key."[7]

Lack of Key Management

The 802.11 standard does not specify mechanisms for WEP key management to automatically generate and distribute new keys periodically. It "depends on an external key management service to distribute data enciphering/deciphering keys."[1] This means that key management is left up the network administrator to manually configure each device. Not only will the administrator have to manually add WEP keys when setting up the WLAN, they will also have to periodically generate a new key and manually configure each AP and STA to propagate the new key to each device. Given the time and headaches it would involve to manually update any more than just a few devices, manual key management is really not a feasible option. This is obviously a major drawback to real network security since once the WLAN is setup it is very likely that the WEP keys will seldom if ever get changed. With the WEP key rarely changing it is for the most part a static key. This only compounds the problems with WEP as stated earlier. If the WEP key is static it simplifies the work that an attacker would have to go through to crack the WEP key. When the WEP key is static an attacker does not have to worry about a shortened period of time to capture network packets to gather the WEP key information before the key is changed. In a secure environment the cryptographic

[7] www.cisco.com
[1] ANSI/IEEE Std 802.11, 1999 Edition

keys needs to be automatically changed at periodic intervals or per session to limit the time any key is used.

Other Authentication Issues

Mutual authentication – both the STA and the AP should be able to authenticate that the other entity is who they claim to be.

Identification and authentication for users – Identification and authentication needs to be tied to an actual user and not just a MAC address or WEP Key.

How the 802.11 Standard Matches Up to Security Principles

Now that the basic operations and security features of the 802.11 standard have been explained we should look at how they apply to the basic security concepts like identity, authentication and authorization.

Identity - "whom someone or what something is"—for example, the name by which one is recognized. This identity may be of a human being, a program, a computer, or data. Identification is the process for establishing whom someone or what something claims to be.[8]

Authentication - is the process of confirming the correctness of the claimed identity.[8]

Authorization - means the approval, permission, or empowerment for someone or something to do something.[8]

Identity in 802.11 is primary confined to the MAC addresses to identify the radio NICs and the SSID to identify the wireless network. While the MAC address works great to identify a wireless NIC in order to know where to send packets to, it does not really identify what is important to network security, the user operating the radio NIC and receiving the packets.

802.11 authentication consists of the null authentication in Open authentication, which is really no authentication at all, and the weak authentication in Shared Key authentication. According to the definition of authentication above, the authentication scheme has to be able to confirm the correctness of the claimed identity. Due to the weakness of both of the 802.11 authentication schemes, it could be said that their ability to securely determine the claimed identity is inadequate for any real network security.

One problem with 802.11 authentication seems to be that, for the most part, one way or another it gives away half of the identification-authentication equation. In a basic security authentication scheme, two elements are required, the user ID and password. The user ID is the identification element and the password is needed for the authentication element. In 802.11 the identification requirements are virtually non-existent since all that is required is a MAC address, which is not tied to a user. The

[8] SANS GSEC Online Training Material

SSID, which could be considered a password is often broadcast over the radio waves in the beacon frames. Even if it is not included in the beacons the SSID is easily sniffed from existing network traffic. While the WEP based Shared Key authentication is better than nothing it is easy enough to break that while not exactly giving the key away, it doesn't take much work to get it.

Authorization in 802.11 is wide open. If you got past the authentication you have access to whatever is available on the network.

802.11 Security Summary

The security issues of the 802.11 standard can be summarized by:

- The inherent physical properties of a WLAN make it more vulnerable to eavesdropping, session hijacking and denial of service attacks.
- Identification relies almost entirely on MAC addresses which can easily be spoofed and is not tied to a user
- The authentication schemes are weak and do not provide a method for mutual authentication
- The WEP cryptographic algorithm that is relied on for privacy is weak and does not provide a good assurance that the data will remain confidential.
- Lack of a key management mechanisms compounds the problem of the weak WEP cryptographic algorithm
- There is no authorization mechanism specified in the 802.11 standard

Due to the inherent weaknesses in the 802.11 standard, by itself cannot be considered secure enough to adequately provide confidentiality, integrity and availability to the WLAN and the systems connected to it.

While the basic 802.11 WLAN may not be as secure as many Network Managers will be able to tolerate it does have some benefits if easy access is important. For instance in the case of Internet cafes where easy connectivity and wide open access are desirable characteristics, then an 802.11 WLAN would be a perfect fit. If network security is a concern at all and an 802.11 WLAN is being considered then the WLAN should implement one or more of the options available to fill in some of the security holes in an 802.11 WLAN.

Options to Supplement the 802.11 Standard WLAN

The majority of the security problems associated with the basic 802.11 WLAN can for the most part be remedied by implementing one or more options to supplement 802.11 WLAN security. The non-proprietary options available or soon to be available are the IEEE 802.1x standard, Wi-Fi Protected Access (WPA) security enhancements, and the soon to be approved IEEE 802.11i Task Group(802.11TGi). Both the WPA and 802.11TGi options make use of the 802.1x specifications in their implementations.

IEEE 802.1x Standard

The IEEE 802.1x standard is defined within the IEEE Std 802.1X-2001 document as the:

> Standard for Local and Metropolitan area Networks: Port-Based Network Access Control.

And has the stated purpose of:

> providing compatible authentication and authorization mechanisms for devices interconnected by IEEE 802 LANs, this standard specifies a general method for the provision of port-based network access control.

Also listed within the scope of the standard is:

> Examples of ports in which the use of authentication can be desirable include the Ports of MAC Bridges (as specified in IEEE 802.1D), the ports used to attach servers or routers to the LAN infrastructure, and associations between stations and access points in IEEE 802.11 Wireless LANs.

[9] IEEE Std 802.1X-2001

The 802.1x standard applies to wired as well as wireless networking. We will focus on how it can be used to improve 802.11 WLAN implementations using the authentication and authorization functions in 802.1x.

The 802.1x standard introduces some new terms and principles that need to be defined to better understand how 802.1x works.

Definitions

"Supplicant: An entity at one end of a point-to-point LAN segment that is being authenticated by an authenticator attached to the other end of that link."[9] In WLAN terms this is the wireless station(STA) or wireless client attempting access through the authenticator AP.

"Authenticator: An entity at one end of a point-to-point LAN segment that facilitates authentication of the entity attached to the other end of that link."[9] This is the 802.1x enabled wireless AP that enforces authentication before allowing access through one of it's controlled ports.

"Authentication Server: An entity that provides an authentication service to an authenticator. This service determines, from the credentials provided by the supplicant, whether the supplicant is authorized to access the services provided by the authenticator."[9] This in most cases is going to be some form of Remote Authentication Dial-In User Service (RADIUS) server.

[9] IEEE Std 802.1X-2001

While 802.1x does not solve all of the 802.11 standard's weaknesses it does significantly improve WLAN security by providing a means for dynamic key management, stronger authentication, MAC access control and authorization services. We will briefly cover some of the important features of 802.1x.

The 802.1x standard is based on the Extensible Authentication Protocol(EAP) which is a transport protocol designed for use over point-to-point network connections. "EAP messages were originally defined to be sent as the payload of PPP frames, the IEEE 802.1X standard defines EAP over LAN (EAPOL), which is a method of encapsulating EAP messages so that they can be sent over Ethernet or wireless LAN segments."[13] EAP allows for several choices of authentication methods including but not limited to, MD5, EAP-TLS, EAP-TTLS, and PEAP. The more secure methods involve the use of public key certificates and the Transport Layer Security (TLS) protocol. Some of the security enhancements gained with the public key certificate/TLS based methods include:

- Mutual authentication – authentication server to supplicant as well as supplicant to authentication server
- Key exchange to establish dynamic WEP\Crypto keys
- Message authentication
- Message encryption

[13] microsoft.com – technet article

With 802.1x the supplicant(STA) is denied access through the authenticator(AP) port until it has been successfully authenticated and authorized by the authentication server. Figure 5 below shows the wireless connection process with the addition of the 802.1x authentication scheme.

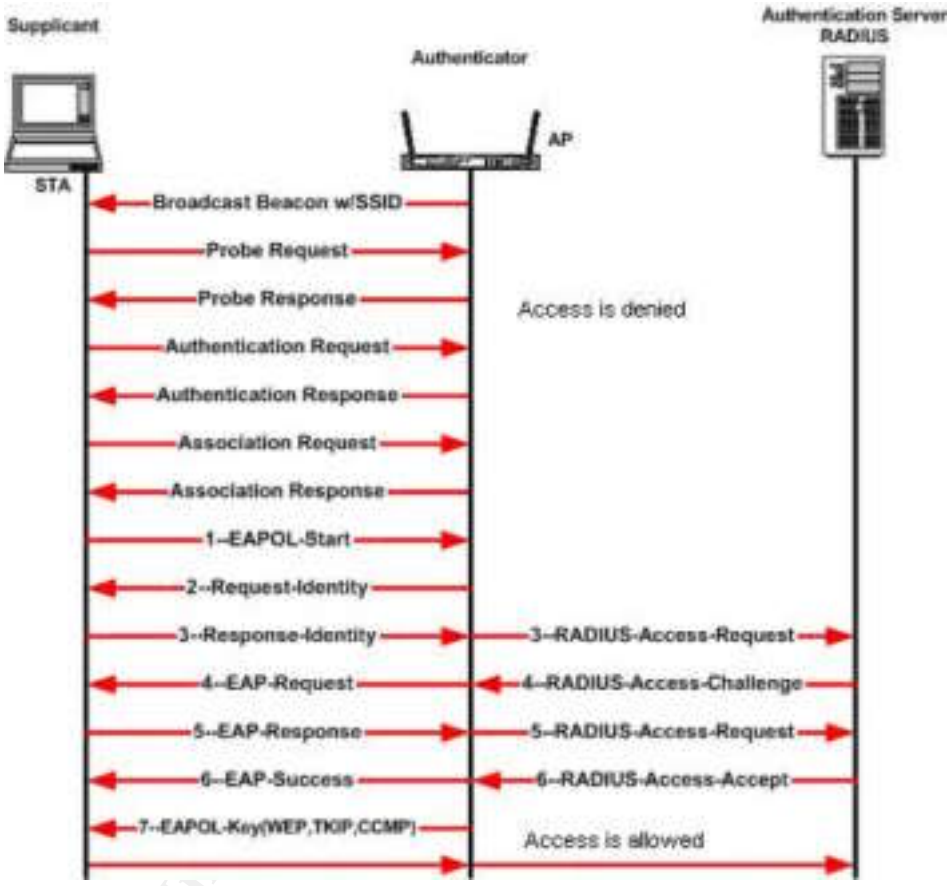

Figure 5 – 802.11 Communications with 802.1x

802.1x and EAP strengthen 802.11 security by providing support for stronger authentication and key management mechanisms. Authentication is improved by including options like per-user identification/authentication, token cards, certificates, smart cards, biometrics, etc. The key management methods add options for dynamic, per-station, per-session key management for key regeneration and distribution. Since the 802.1x standard is not an 802.11 wireless specific standard, 802.1x does not specify a replacement for the WEP cryptographic algorithm. The next two options for improving WLAN security do implement replacements for WEP.

WPA - Wi-Fi Protected Access

The IEEE 802.11TGi is expected to be the long-term solution to the weaknesses associated with WEP and 802.11. However 802.11TGi is not an approved standard as of yet. The nonprofit trade organization Wi-Fi Alliance working with the IEEE has crafted an interim solution in WPA meant to enhance WLAN security through software upgrades on existing hardware. "The WPA specification is a subset of the current 802.11i draft, and will be forward compatible with the upcoming IEEE 802.11i standard."[10]

"To improve data encryption, WPA utilizes its Temporal Key Integrity Protocol (TKIP). TKIP provides important data encryption enhancements including a per-packet key mixing function, a message integrity check (MIC) named *Michael*, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism."[10]

An April, 2003 Wi-Fi Alliance Whitepaper gives the following description of TKIP and MIC:

> TKIP replaces WEP's single static key with keys that are dynamically generated and distributed by the authentication server. TKIP uses a key hierarchy and key management methodology that removes the predictability which intruders relied upon to exploit the WEP key. To do this, TKIP leverages the 802.1X/EAP framework. The authentication server, after accepting a user's credentials, uses 802.1X to produce a unique master, or "pair-wise" key for that computing session. TKIP distributes this key to the client and the AP and sets up a key hierarchy and management system, using the pairwise key to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated during that user's session. TKIP's key hierarchy exchanges WEP's single static key for some 500 trillion possible keys that can be used on a given data packet.
>
> The Message Integrity Check (MIC) is designed to prevent an attacker from capturing data packets, altering them and resending them. The MIC provides a strong mathematical function in which the receiver and the transmitter each compute and then compare the MIC. If they do not match, the data is assumed to have been tampered with and the packet is dropped.

[11] Wi-Fi Alliance – WPA Whitepaper

To strengthen user authentication, WPA implements 802.1x and EAP.

In a small networking environment, where there are no authentication servers or EAP framework, WPA can be used in Pre-Shared Key (PSK) mode. This allows the use of a manually entered key or password also called a master key in the AP and on each STA

[10] Wi-Fi Alliance – WPA Overview
[11] Wi-Fi Alliance – WPA Whitepaper

on the WLAN. WPA takes over automatically from that point and kicks off the TKIP encryption process.

IEEE 802.11TGi

The IEEE 802.11TGi presents a long term solution to the weaknesses in the 802.11 standard. The 802.11i standard will use of the stronger cryptographic algorithm Advanced Encryption Standard(AES) which presents a vast improvement over the original 802.11 WEP algorithm. Due to the use of AES, most current WLAN equipment will need to be replaced to be able to handle the AES processing.

The 802.11i standard will contain many of the same features as WPA and also have some additional specifications for AES data privacy protocols.

The IEEE 802.11i Overview[12] describes the 802.11i standard's data privacy options:

IEEE 802.11TGi defines three data privacy protocols:

CCMP - Based on AES in CCM mode - Counter-Mode/CBC-MAC protocol
WRAP - Wireless Robust Authenticated Protocol (AES-OCB)
TKIP – Temporal Key Integrity Protocol, legacy support

- Can be implemented in software
- Reuses existing WEP hardware
- Runs WEP as a sub-component

802.11i Key Management
Key Hierarchy - Pairwise Key Hierarchy and Group Key Hierarchy

([12] IEEE 802.11i Overview)

Additional specifications will be included in 802.11i such as secure IBSS, secure fast handoff, and secure de-authentication and disassociation that are not included in WPA.

The 802.11TGi specifications include many of the same security improvements as those found in WPA. One of the important differences between WPA and 802.11TGi is that 802.11TGi provides a real replacement for the original WEP algorithm using AES based protocols. The 802.11TGi is expected to become an approved IEEE standard very soon and should be widely accepted among wireless equipment vendors. The one drawback is, as stated before that the inclusion of AES encryption will require higher processing requirements and new WLAN hardware.

[12] IEEE 802.11i Overview

802.11 Improvements with 801.1x, WPA and 802.11i

It may helpful to compare the problems found in the original 802.11 standard with the solutions offered in 801.1x and WPA/802.11i to better understand how 802.11 security has been improved with these options. Table 1 compares 802.11 issues with how they have been resolved in 802.1x, WPA and 801.1TGi:

802.11 Security Issues	801.1x	WPA	801.11i
Identification – tied to MAC only	Can tie identification to a user via user ID, certificate, smartcard, etc.	Uses 802.1x	Uses 802.1x
Authentication – weak-null Open, SKA tied to WEP	Uses an authenticator to block access through port until authenticated by authentication server, uses EAP-no clear text authentication traffic to sniff,	Uses 802.1x, uses TKIP to strengthen cryptography	Uses 802.1x, replaces WEP with AES based CCMP and WRAP
Authentication – no mutual authentication	Provides mutual authentication – supplicant to authentication server and authentication server to supplicant	Uses 802.1x	Uses 802.1x
WEP – easy to crack, uses same key for all activity		Uses RC4 based TKIP- per-packet key mixing, message integrity checking , re-keying mechanism	Uses AES based CCMP and WRAP as a replacement for WEP, also uses TKIP
No automated Key Management functionality	EAP - provide support for secure transport for key management	Uses RC4 based TKIP- per-packet key mixing, message integrity checking, re-keying mechanism	Uses AES based CCMP and WRAP as a replacement for WEP, also uses TKIP, uses Pairwise and Group Key Hierarchy
No Authorization mechanism	Authorization by blocking port access for the supplicant until the authentication server verifies user(supplicant) credentials in RADIUS and informs the authenticator to allow access		

Table 1 – Comparing 802.11 Security Issues with Solutions

The addition of the 802.1x, WPA and 802.11i features to an 802.11 WLAN help to increase the security posture to acceptable levels. The 802.1x features help to strengthen the identification, authentication and authorization elements for better overall network security. Using WPA and 802.11i in conjunction with 802.1x to replace the weak WEP encryption and implement an automated key management scheme vastly improves the confidentiality aspects of network security for the WLAN. With these added security features a WLAN could be considered reasonably secure and able to

provide adequate levels of confidentiality, integrity and availability. Although the availability may still be somewhat vulnerable due the inherent nature of a WLAN being easier to access and can be sent bogus transmissions to the point of causing availability issues.

Overview

While the original 802.11 standard is a boon to easy connectivity and open access it suffers from a lack of real network security capabilities. An 802.11 WLAN's security profile can be improved by using 801.1x, WPA, and in the future, the 802.11i standard.

A WLAN configured with the only the default 802.11 standard security specifications is considered very insecure and should be limited to use on networks where information security is of no concern. Coffee shops where the only function of the WLAN is to provide wide-open, easy Internet access would be an appropriate use of a generic 802.11 WLAN. Using WPA and the upcoming 801.11i standard in conjunction with 801.1x to secure most of the gapping security holes found in 802.11 should bring an 802.11 WLAN security up to acceptable levels for most computing environments. Even with 802.1x, WPA and 802.1i in place it would be prudent to treat a WLAN as an untrusted network and ensure that the proper firewalls and/or VPNs are in place to protect the wired network. An 802.11 WLAN employing 802.1x and WPA/802.11i provides a good balance of the benefits of wireless networking and information security.

References:

1. "ANSI/IEEE Std 802.11, 1999 Edition" Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications
URL: http://www.cs.unc.edu/~lindsey/7ds/notes/802.11/802.11-1999.pdf (16 Dec. 2003)

2. Geier, Jim. "802.11 Beacons Revealed" (31 October, 2002)
URL: http://www.wi-fiplanet.com/tutorials/article.php/1492071 (16 Dec. 2003)

3. Geier, Jim. "Understanding 802.11 Frame Types" (15 August, 2002)
URL: http://www.wi-fiplanet.com/tutorials/print.php/1447501 (16 Dec. 2003)

4. Geier, Jim. "802.11 MAC Layer Defined" (4 June 2002)
URL: http://www.wi-fiplanet.com/tutorials/print.php/1216351 (16 Dec. 2003)

5. CIRT.net "Default Wireless Configurations"
URL: http://www.cirt.net/cgi-bin/ssids.pl (16 Dec. 2003)

6. Kismet – Home Page
URL: http://www.kismetwireless.net (16 Dec. 2003)

7. Convery, Sean. Miller, Darrin. Sundaralingam, Sri. "Cisco SAFE: Wireless LAN Security in Depth"
URL: http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safwl_wp.pdf (16 Dec. 2003)

8. SANS GSEC Online Training material. "Defense in-Depth" SANS Security Essentials II Section 2, Chapter 7
file: SECBK_21_1102.pdf February 2003 (2003) 298

9. "IEEE Std 802.1X-2001" IEEE Standard for Local and metropolitan area networks-Port-Based Network Access Control
URL: http://standards.ieee.org/getieee802/download/802.1X-2001.pdf (16 Dec. 2003)

10. Wi-Fi Alliance. "Overview Wi-Fi Protected Access" (15 Oct. 2002)
URL: http://www.weca.net/OpenSection/pdf/Wi-Fi_Protected_Access_Overview.pdf (16 Dec. 2003)

11. Wi-Fi Alliance. "Wi-Fi Protected Access: Strong, standards-based, interoperable security for today's Wi-Fi networks" (29 April 2003)
URL: http://www.weca.net/OpenSection/pdf/Whitepaper_Wi-Fi_Security4-29-03.pdf (16 Dec. 2003)

12. Cam, Nancy. Moore, Tim. Stanley, Dorothy. Walker, Jesse. "IEEE 802.11i Overview"
URL: http://csrc.nist.gov/wireless/S10_802.11i%20Overview-jw1.pdf (16 Dec. 2003)

13. "The Cable Guy - April 2002" IEEE 802.1X Authentication for Wireless Connections (April 2002)
URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/columns/cableguy/cg0402.asp (16 Dec. 2003)