WIRELESS LAN 802.11 SECURITY

Hasan – Al – Banna
Student ID: 03101078

Riaz Mahmood Rajib
Student ID: 03101060

A Thesis
Presented to
The Faculty of the
Department of Computer Science & Engineering

In Partial Fulfillment of the
Requirements for the Degree
of
Bachelor of Science (BS) in Computer Science & Engineering
January 2008

DECLARATION

I hereby declare that this thesis is based on the results found by myself. Materials of work found by other researcher are mentioned by reference. This thesis, neither in whole nor in part, has been previously submitted for any degree.

Signature of Supervisor	Signature of Author

Abstract

When the wireless communications is coming to the offices and the homes, there are some new security issues to be taken care of. Today we have continuously growing markets for the wireless LANs, but there is big black hole in the security of this kind of networks. Companies without controlled doors cannot ensure the security and safety of their employees, nor can they prevent piracy and theft. Networks without controlled access cannot guarantee the security or privacy of stored data, nor can they keep network resources from being exploited by hackers. In our thesis we are giving an overview of the security functions and threats specified in one wireless LAN standard, namely in the IEEE 802.11.

The IEEE 802.11 is one of the very first wireless local area network standards that is currently widely deployed. Much research has been done on the IEEE 802.11 wireless network standard and the standard is known for its insecurity. Several reports have addressed the 802.11-based network vulnerabilities mainly for its lack of authentication.

This thesis aims to improve the IEEE 802.11 standard by analyzing the security mechanisms the standard provides. The IEEE 802.11 standard provides basic security mechanisms such as the wired equivalent protocol, an encryption protocol, and the media access based access control list, which is essentially a list of legitimate clients. Attackers may easily penetrate these IEEE 802.11 basic security mechanisms.

I did not perform any testing of the attack solutions. Successors of this thesis project should implement the attack and test out solutions.

ACKNOWLEDGEMENTS

We would like to thank our supervisor Ms. Sadia Hamid Kazi for her support and assistance in the preparation of this thesis. In addition, special thanks are due to Mr. Risat Mahmud Pathan , whose familiarity with the subject of Wireless Security was invaluable.

TABLE OF CONTENTS

1. Introduction to Thesis Project

The Internet boom during the 20th century created much commercial opportunities for organizations. From the early Internet access technologies of modem dial-ups to Digital Subscriber Lines or cable modems, the fast improvement of the Internet has never ceased. As the speed of Internet access increases, people began to focus on improving the mobility and portability of computers accessing the Internet. Most organizations now deploy wireless local area networks (WLAN) as a convenient way of providing Internet access . WLANs differ from the normal local area networks mainly in WLAN’s ability to use radio signals as opposed to physical wires to transmit data. A major problem with transmitting data as radio frequencies resides in the fact that they are easy to intercept. Any computer with WLAN accessible hardware is capable of intercepting data transmitted by another computer in the same network. This thesis project reviews the security of the IEEE 802.11 WLAN standard and analyses different types of wireless attack and techniques. The goal of this thesis project is to give some countermeasures against these attacks to increase the overall security of the WLAN environment.

1.1 Problems with IEEE 802.11, the Wireless Network Standard

The Institute of Electrical and Electronics Engineers (IEEE) is a non-profit association that “aims to advance global prosperity by fostering technological innovation, enabling members' careers and promoting community world-wide” (IEEE Website). The IEEE standards are to unify hardware designs for technologies such as the Internet; IEEE 802.11 is one of the earliest WLAN standards defined. The IEEE 802.11 standard has several known problems exploited. The standard is ‘weak’ in the sense that it does not provide data encryption for authentication nor association. Through authentication, computers are able to identify who they are, and through association, computers connect to an access point (AP), or a device that is physically connected to some outside networks. Without data encryption in the authentication data or association data sent, attackers can easily deceive access points to gain illegal access. Attackers may also generate a series of dis-authentication or dis-association messages to bring down the whole network .

1.2 Method and Approach to Solve the Problem

One of the most straightforward approaches to fixing a poorly designed standard is to come up with newer standards. Currently there are several new standards deployed for WLANs. Although organizations can always invent new standards to counter existing flaws, the phase of converting from an older standard to a newer one will take a substantial amount of time. Currently the 802.11 and 802.11b standards are already widely deployed. Changing to a newer standard will require hardware changes, adding cost to an organization that tries to adopt the newer standards. The approach that this thesis takes is to examine all the current and future standards. Other than reviewing the

802.11 standard, this thesis project also focuses on the Wireless attacks and the recommended solutions.
This thesis project offers an introduction to WLAN standards, an overview of WLAN security, and an discussion of wireless attacks. The impacts of this project will be concentrated on the social, economic, and ethical side.

1.3 Social, Economic, and Ethical Impacts

This fundamental goal of this thesis project is to improve the WLAN Internet accessing environment by pointing out security flaws and suggesting solutions to them. Organizations that choose or have already chosen to deploy WLAN should consider the current existing problems. The impact of this thesis will hopefully bring awareness to the community about the capabilities that a WLAN attacker may obtain. The project seeks to allow readers to perceive how attackers may undertake the attacks, and then analyzes each attack. The defense solution offered against some of the WLAN attacks will provide a more secure Internet accessing environment. The social benefits of this project are not limited to only providing a better and secure environment, but may also benefit the economy. Every year companies lose a fair amount of money due to security breaches such as computer viruses and Internet attacks. The valuable data that companies store on corporate databases, namely enterprise servers, may accumulate to several billions of dollars. This thesis project may provide another layer of protection to those data, impacting on the economy as a whole .

The rise in the field of Internet Security has also created business opportunities. The company Symantec, for example, bases their revenue on providing Internet security related services. With the analysis provided by this thesis project, the expectation and the most desired situation is to discourage Internet attackers from performing any attacks. Organizations world wide have considered Internet attacking unethical and in several countries it is a violation of the law
.

1.4 Why Do We Need Wireless Network?

The major difference between WLAN and a normal local area network (LAN) is the ability that WLAN users have superior mobility. WLAN users may move with their laptops from place to place, yet still can obtain Internet Access. LAN users, on the other hand, are restrained to physical wires and the architecture of their buildings. Disadvantages of WLANs as opposed to wired LANs are in WLAN’s speed and security. WLANs have signals that are much easier to intercept (via air). WLANs also have a slower transmission rate, although this may not always be the case as newer versions of WLANs are comparable to LANs. The questions arise: why do we need WLANs? Is mobility really a substantial issue? By deploying WLANs, organizations have sacrificed security for mobility. Although Internet Security problems with WLANs continue to emerge through time, the deployment of WLANs has not decreased. “By 2006, research firm Gartner expects 99 million WiFi users and 89,000 public WiFi access points around the world.” This proves the need and desire for a safer and a better WLAN environment.

2. Wireless Local Area Networks 802.11

2.1 Introduction to 802.11

Wireless LAN technology is rapidly becoming a crucial component of computer networks and is growing by leaps and bounds. Thanks to the finalization of the IEEE 802.11 wireless LAN standard, wireless technology has emerged from the world of proprietary implementations to become an open solution for providing mobility as well as essential network services where wire line installations proved impractical. The inclusion of the newer IEEE 802.11a and 802.11b versions of the standard offers a firm basis for high-performance wireless LANs. Now companies and organizations are investing in wireless networks at a higher rate to take advantage of mobile, real-time access to information.

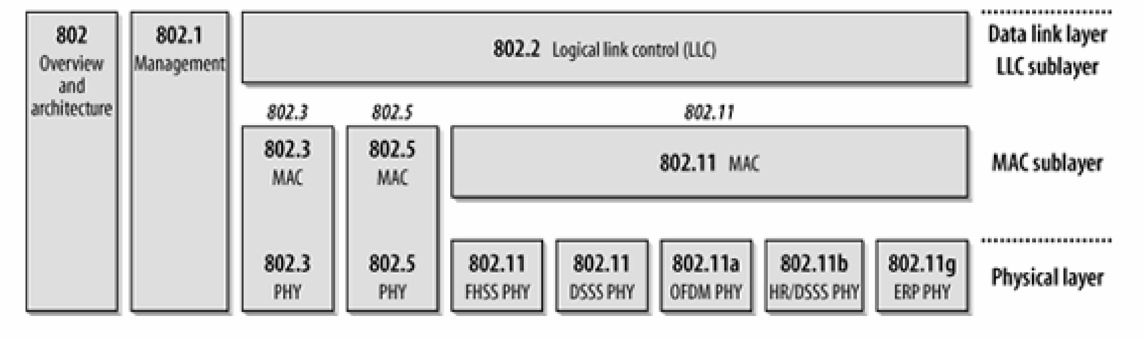
Most wireless LAN suppliers now have 802.11-compliant products, allowing companies to realize wireless network applications based on open systems. The move toward 802.11 standardization is lowering prices and enabling multivendor wireless LANs to interoperate. This is making the implementation of wireless networks more feasible than before, creating vast business opportunities for system implementation companies and consultants. However, many end user companies and system integrators have limited knowledge and experience in developing and implementing wireless network systems. In many cases, there is also confusion over the capability and effectiveness of the 802.11 standard.

The implementation of wireless networks is much different than that of traditional wired networks. In contrast to ethernet, a wireless LAN has a large number of setup parameters that affect the performance and interoperability of the network. An engineer designing the network and the person installing the network must understand these parameters and how they affect the network.

2.2 IEEE 802 Network Technology Family Tree

802.11 is a member of the IEEE 802 family, which is a series of specifications for local area network (LAN) technologies. Figure 2-1 shows the relationship between the various components of the 802 family and their place in the OSI model.

Figure 2-1. The IEEE 802 family and its relation to the OSI model



IEEE 802 specifications are focused on the two lowest layers of the OSI model because they incorporate both physical and data link components. All 802 networks have both a MAC and a Physical (PHY) component. The MAC is a set of rules to determine how to access the medium and send data, but the details of transmission and reception are left to the PHY.

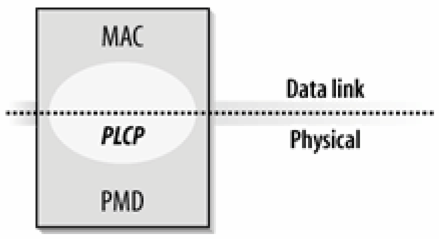
Individual specifications in the 802 series are identified by a second number. For example, 802.3 is the specification for a Carrier Sense Multiple Access network with Collision Detection (CSMA/CD), which is related to (and often mistakenly called) Ethernet, and 802.5 is the Token Ring specification. Other specifications describe other parts of the 802 protocol stack. 802.2 specifies a common link layer, the Logical Link Control (LLC), which can be used by any lower-layer LAN technology. Management features for 802 networks are specified in 802.1. Among 802.1's many provisions are bridging (802.1D) and virtual LANs, or VLANs (802.1Q).

802.11 is just another link layer that can use the 802.2/LLC encapsulation. The base 802.11 specification includes the 802.11 MAC and two physical layers: a frequency-hopping spread-spectrum (FHSS) physical layer and a direct-sequence spread-spectrum (DSSS) link layer. Later revisions to 802.11 added additional physical layers. 802.11b specifies a high-rate direct-sequence layer (HR/DSSS); products based on 802.11b hit the marketplace in 1999 and was the first mass-market PHY. 802.11a describes a physical layer based on orthogonal frequency division multiplexing (OFDM); products based on 802.11a were released as the first edition of this book was completed. 802.11g is the newest physical layer on the block. It offers higher speed through the use of OFDM, but with backwards compatibility with 802.11b. Backwards compatibility is not without a price, though. When 802.11b and 802.11g users coexist on the same access point, additional protocol overhead is required, reducing the maximum speed for 802.11g users.

To say that 802.11 is "just another link layer for 802.2" is to omit the details in the rest of this book, but 802.11 is exciting precisely because of these details. 802.11 allows for mobile network access; in accomplishing this goal, a number of additional features were incorporated into the MAC. As a result, the 802.11 MAC may seem baroquely complex compared to other IEEE 802 MAC specifications.

The use of radio waves as a physical layer requires a relatively complex PHY, as well. 802.11 splits the PHY into two generic PMcomponents: the Physical Layer Convergence Procedure (PLCP), to map the MAC frames onto the medium, and a Physical Medium Dependent (PMD) system to transmit those frames. The PLCP straddles the boundary of the MAC and physical layers, as shown in Figure 2-2. In 802.11, the PLCP adds a number of fields to the frame as it is transmitted "in the air."

Figure 2-2. PHY components

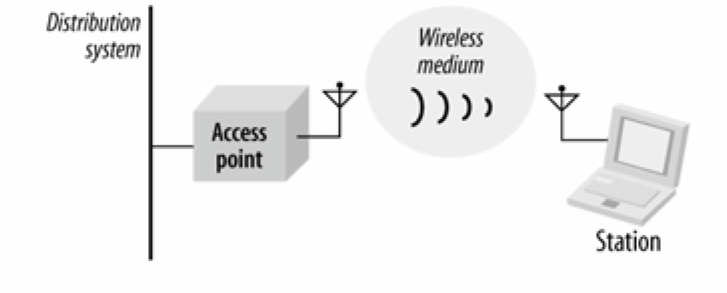


All this complexity begs the question of how much you actually need to know. As with any technology, the more you know, the better off you will be. The 802.11 protocols have many knobs and dials that you can tweak, but most 802.11 implementations hide this complexity. Many of the features of the standard come into their own only when the network is congested, either with a lot of traffic or with a large number of wireless stations. Networks are increasingly pushing the limits in both respects.

2.3 802.11 Nomenclature and Design

802.11 networks consist of four major physical components, which are summarized in Figure 2-3.

Figure 2-3. Components of 802.11 LANs



The components are:

Stations

Networks are built to transfer data between stations. Stations are computing devices with wireless network interfaces. Typically, stations are battery-operated laptop or handheld computers. There is no reason why stations must be portable computing devices, though. In some environments, wireless networking is used to avoid pulling new cable, and desktops are connected by wireless LANs. Large open areas may also benefit from wireless networking, such as a manufacturing floor using a wireless LAN to connect components. 802.11 is fast becoming a de facto standard for linking together consumer electronics. Apple's AirPort Express connects computers to stereos via 802.11. TiVos can connect to wireless networks. Several consumer electronics companies have joined the 802.11 working group, apparently with the intent of enabling high-speed media transfers over 802.11.

Access points

Frames on an 802.11 network must be converted to another type of frame for delivery to the rest of the world. Devices called access points perform the wireless-to-wired bridging function. (Access points perform a number of other functions, but bridging is by far the most important.) Initially, access point functions were put into standalone devices, though several newer products are dividing the 802.11 protocol between "thin" access points and AP controllers.

Wireless medium

To move frames from station to station, the standard uses a wireless medium. Several different physical layers are defined; the architecture allows multiple physical layers to be developed to support the 802.11 MAC. Initially, two radio frequency (RF) physical layers and one infrared physical layer were standardized, though the RF layers have proven far more popular. Several additional RF layers have been standardized as well.

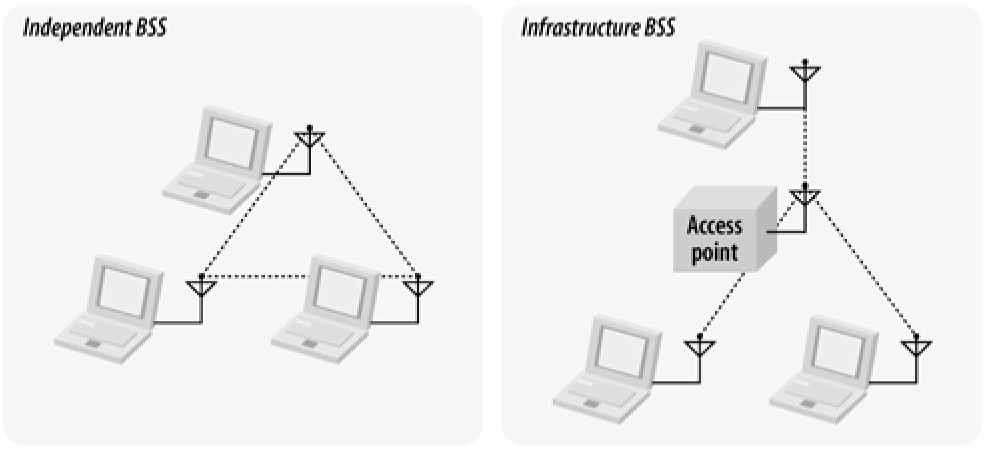
Distribution system

When several access points are connected to form a large coverage area, they must communicate with each other to track the movements of mobile stations. The distribution system is the logical component of 802.11 used to forward frames to their destination. 802.11 does not specify any particular technology for the distribution system. In most commercial products, the distribution system is implemented as a combination of a bridging engine and a distribution system medium, which is the backbone network used to relay frames between access points; it is often called simply the backbone network. In nearly all commercially successful products, Ethernet is used as the backbone network technology.

2.3.1 Types of Networks

The basic building block of an 802.11 network is the basic service set (BSS), which is simply a group of stations that communicate with each other. Communications take place within a somewhat fuzzy area, called the basic service area, defined by the propagation characteristics of the wireless medium.When a station is in the basic service area, it can communicate with the other members of the BSS. BSSs come in two flavors, both of which are illustrated in Figure 2-4.

Figure 2-4. Independent and infrastructure BSSs



2.3.1.1 Independent networks

On the left is an independent BSS (IBSS). Stations in an IBSS communicate directly with each other and thus must be within direct communication range. The smallest possible 802.11 network is an IBSS with two stations. Typically, IBSSs are composed of a small number of stations set up for a specific purpose and for a short period of time. One common use is to create a short-lived network to support a single meeting in a conference room. As the meeting begins, the participants create an IBSS to share data. When the meeting ends, the IBSS is dissolved. Due to their short duration, small size, and focused purpose, IBSSs are sometimes referred to as ad hoc BSSs or ad hoc networks.

2.3.1.2 Infrastructure networks

On the right side of Figure 2-4 is an infrastructure BSS. (To avoid overloading the acronym, an infrastructure BSS is never called an IBSS). Infrastructure networks are distinguished by the use of an access point. Access points are used for all communications in infrastructure networks, including communication between mobile nodes in the same service area. If one mobile station in an infrastructure BSS needs to communicate with a second mobile station, the communication must take two hops. First, the originating mobile station transfers the frame to the access point. Second, the access point transfers the frame to the destination station. With all communications relayed through an access point, the basic service area corresponding to an infrastructure BSS is defined by the points in which transmissions from the access point can be received. Although the multihop transmission takes more transmission capacity than a directed frame from the sender to the receiver, it has two major advantages:

- An infrastructure BSS is defined by the distance from the access point. All mobile stations are required to be within reach of the access point, but no restriction is placed on the distance between mobile stations themselves. Allowing direct communication between mobile stations would save transmission capacity but at the cost of increased physical layer complexity because mobile stations would need to maintain neighbor relationships with all other mobile stations within the service area.
- Access points in infrastructure networks are in a position to assist with stations attempting to save power. Access points can note when a station enters a power-saving mode and buffer frames for it. Battery-operated stations can turn the wireless transceiver off and power it up only to transmit and retrieve buffered frames from the access point.

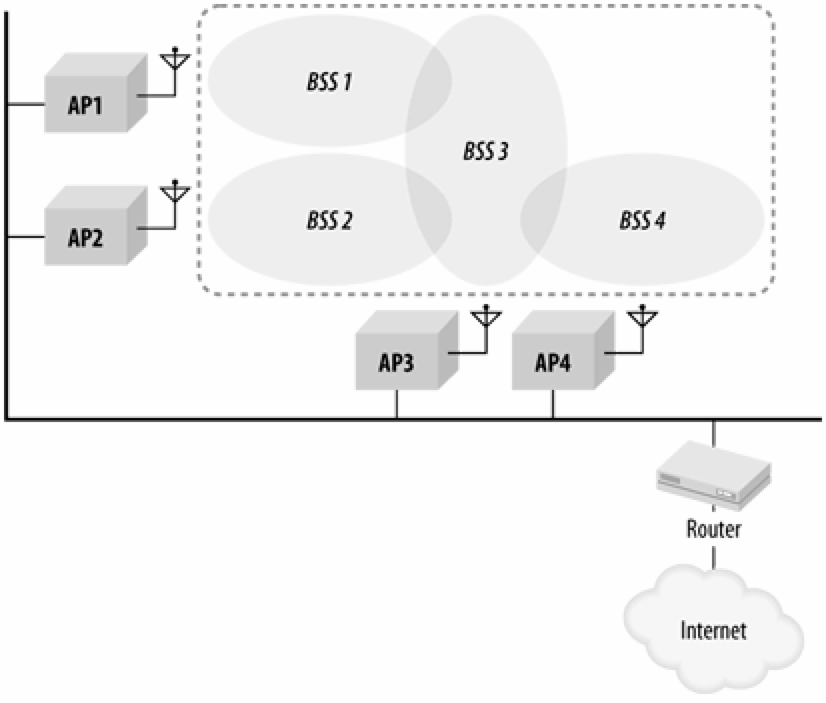
In an infrastructure network, stations must associate with an access point to obtain network services. Association is the process by which mobile station joins an 802.11 network; it is logically equivalent to plugging in the network cable on an Ethernet. It is not a symmetric process. Mobile stations always initiate the association process, and access points may choose to grant or deny access based on the contents of an association request. Associations are also exclusive on the part of the mobile station: a mobile station can be associated with only one access point. The 802.11 standard places no limit on the number of mobile stations that an access point may serve. Implementation considerations may, of course, limit the number of mobile stations an access point may serve. In practice, however, the relatively low throughput of wireless networks is far more likely to limit the number of stations placed on a wireless network.

2.3.1.3 Extended service areas

BSSs can create coverage in small offices and homes, but they cannot provide network coverage to larger areas. 802.11 allows wireless networks of arbitrarily large size to be created by linking BSSs into an extended service set (ESS). An ESS is created by chaining BSSs together with a backbone network. All the access points in an ESS are given the same service set identifier (SSID), which serves as a network "name" for the users.

802.11 does not specify a particular backbone technology; it requires only that the backbone provide a specified set of services. In Figure 2-5, the ESS is the union of the four BSSs (provided that all the access points are configured to be part of the same ESS). In real-world deployments, the degree of overlap between the BSSs would probably be much greater than the overlap in Figure 2-5. In real life, you would want to offer continuous coverage within the extended service area; you wouldn't want to require that users walk through the area covered by BSS3 when en route from BSS1 to BSS2.

Figure 2-5. Extended service set



Stations within the same ESS may communicate with each other, even though these stations may be in different basic service areas and may even be moving between basic service areas. For stations in an ESS to communicate with each other, the wireless medium must act like a single layer 2 connection. Access points act as bridges, so direct communication between stations in an ESS requires that the backbone network also look like a layer 2 connection. First-generation access points required direct layer 2 connections through hubs or virtual LANs; newer products implement a variety of tunneling technologies to emulate the layer 2 environment.

Extended service areas are the highest-level abstraction supported by 802.11 networks. Access points in an ESS operate in concert to allow the outside world to use the station's MAC address to talk to a station no matter what its location is within the ESS. In Figure 2-5, the router uses the station's MAC address as the destination to deliver frames to a mobile station; only the access point with which that mobile station is associated delivers the frame. The router remains ignorant of the location of the mobile station and relies on the access points to deliver the frame.

2.3.1.4 Multi-BSS environments: "virtual APs"

Early 802.11 radio chips had the ability to create a single basic service set. An AP could have connect users to only one "wireless network," and all users on that network had similar, if not identical, privileges. In early deployments with limited user counts, a single logical network was sufficient. As wireless networking grew in popularity, one network no longer sufficed.

As an example, most organizations get regular visitors, many of whom have 802.11 equipment and need (or strongly desire) Internet access. Guests are not trusted users. One common way of coping with guest access is to create two extended service sets on the same physical infrastructure. Current 802.11 chipsets can create multiple networks with the same radio. Using modern chipsets, each access point hardware device can create two BSSs, one for the network named guest, and one for the network named internal. Within the AP, each SSIDs is associated with a VLAN. The guest network is connected to a VLAN prepared for public access by unknown and untrusted users, and is almost certainly attached outside the firewall.

Wireless devices see two separate networks in the radio domain, and can connect to whatever one suits their needs. (Naturally, the internal network is probably protected by authentication prevent unauthorized use.) Users who connect to the wireless network named guest will be placed on the guest VLAN, while users who connect to the wireless network named internal will be authenticated and placed on the internal network.

This somewhat contrived example illustrates the development of what many call virtual access points. Each BSS acts like its own self-contained AP, with its own ESSID, MAC address, authentication configuration, and encryption settings. Virtual APs are also used to create parallel networks with different security levels. Current 802.11 radio chipsets have the ability to create 32 or even 64 BSSes, which is adequate for nearly every configuration.

2.4 802.11 Network Operations

From the outset, 802.11 was designed to be just another link layer to higher-layer protocols. Network administrators familiar with Ethernet will be immediately comfortable with 802.11. The shared heritage is deep enough that 802.11 is sometimes referred to as "wireless Ethernet."

The core elements present in Ethernet are present in 802.11. Stations are identified by 48-bit IEEE 802 MAC addresses. Conceptually, frames are delivered based on the MAC address. Frame delivery is unreliable, though 802.11 incorporates some basic reliability mechanisms to overcome the inherently poor qualities of the radio channels it uses

From a user's perspective, 802.11 might just as well be Ethernet. Network administrators, however, need to be conversant with 802.11 at a much deeper level. Providing MAC-layer mobility while following the path blazed by previous 802 standards requires a number of additional services and more complex framing.

2.4.1 Network Services

One way to define a network technology is to define the services it offers and allow equipment vendors to implement those services in whatever way they see fit. 802.11 provides nine services. Only three of the services are used for moving data; the remaining six are management operations that allow the network to keep track of the mobile nodes and deliver frames accordingly.

The services are described in the following list and summarized in Table 2-1:

Distribution

> This service is used by mobile stations in an infrastructure network every time they send data. Once a frame has been accepted by an access point, it uses the distribution service to deliver the frame to its destination. Any communication that uses an access point travels through the distribution service, including communications between two mobile stations associated with the same access point.

Integration

> Integration is a service provided by the distribution system; it allows the connection of the distribution system to a non-IEEE 802.11 network. The integration function is specific to the distribution system used and therefore is not specified by 802.11, except in terms of the services it must offer.

Association

Delivery of frames to mobile stations is made possible because mobile stations register, or associate, with access points. The distribution system can then use the registration information to determine which access point to use for any mobile station. Unassociated stations are not "on the network," much like workstations with unplugged Ethernet cables. 802.11 specifies the function that must be provided by the distribution system using the association data, but it does not mandate any particular implementation. When robust security network protocols are in use, association is a precursor to authentication. Prior to the completion of authentication, an access point will drop all network protocol traffic from a station.

Reassociation

When a mobile station moves between basic service areas within a single extended service area, it must evaluate signal strength and perhaps switch the access point with which it is associated. Reassociations are initiated by mobile stations when signal conditions indicate that a different association would be beneficial; they are never initiated directly by the access point. (Some APs will kick stations off in order to force a client into being the reassociation process; in the future, reassociation may be more dependent on the infrastructure with the development of better network management standards.)

After the reassociation is complete, the distribution system updates its location records to reflect the reachability of the mobile station through a different access point. As with the association service, a robust security network will drop network protocol traffic before the successful completion of authentication.

Disassociation

To terminate an existing association, stations may use the disassociation service. When stations invoke the disassociation service, any mobility data stored in the distribution system is removed. Once disassociation is complete, it is as if the station is no longer attached to the network. Disassociation is a polite task to do during the station shutdown process. The MAC is, however, designed to accommodate stations that leave the network without formally disassociating.

Authentication

Physical security is a major component of a wired LAN security solution. Network attachment points are limited, often to areas in offices behind perimeter access control devices. Network equipment can be secured in locked wiring closets, and data jacks in offices and cubicles can be connected to the network only when needed. Wireless networks cannot offer the same level of physical security, however, and therefore must depend on additional authentication routines to ensure that users accessing the network are authorized to do so. Authentication is a necessary prerequisite to association because only authenticated users are authorized to use the network.

Authentication may happen multiple times during the connection of a client to a wireless network. Prior to association, a station will perform a basic identity exchange with an access point consisting of its MAC address. This exchange is often referred to as "802.11" authentication, which is distinct from the robust cryptographic user authentication that often follows.

De-authentication

Deauthentication terminates an authenticated relationship. Because authentication is needed before network use is authorized, a side effect of deauthentication is termination of any current association. In a robust security network, deauthentication also clears keying information.

Confidentiality

Strong physical controls can prevent a great number of attacks on the privacy of data in a wired LAN. Attackers must obtain physical access to the network medium before attempting to eavesdrop on traffic. On a wired network, physical access to the network cabling is a subset of physical access to other computing resources. By design, physical access to wireless networks is a comparatively simpler matter of using the correct antenna and modulation methods.

In the initial revision of 802.11, the confidentiality service was called privacy, and provided by the now-discredited Wired Equivalent Privacy (WEP) protocol. In addition to new encryption schemes, 802.11i augments the confidentiality service by providing user-based authentication and key management services, two critical issues that WEP failed to address.

MSDU delivery

Networks are not much use without the ability to get the data to the recipient. Stations provide the MAC Service Data Unit (MSDU) delivery service, which is responsible for getting the data to the actual endpoint.

Transmit Power Control (TPC)

TPC is a new service that was defined by 802.11h. European standards for the 5 GHz band require that stations control the power of radio transmissions to avoid interfering with other users of the 5 GHz band. Transmit power control also helps avoid interference with other wireless LANs. Range is a function of power; high transmit power settings make it more likely that a client's greater range will interfere with a neighboring network. By controlling power to a level that is "just right," it is less likely that a station will interfere with neighboring stations.

Dynamic Frequency Selection (DFS)

Some radar systems operate in the 5 GHz range. As a result, some regulatory authorities have mandated that wireless LANs must detect radar systems and move to frequencies that are not in use by radar. Some regulatory authorities also require uniform use of the 5 GHz band for wireless LANs, so networks must have the ability to re-map channels so that usage is equalized.

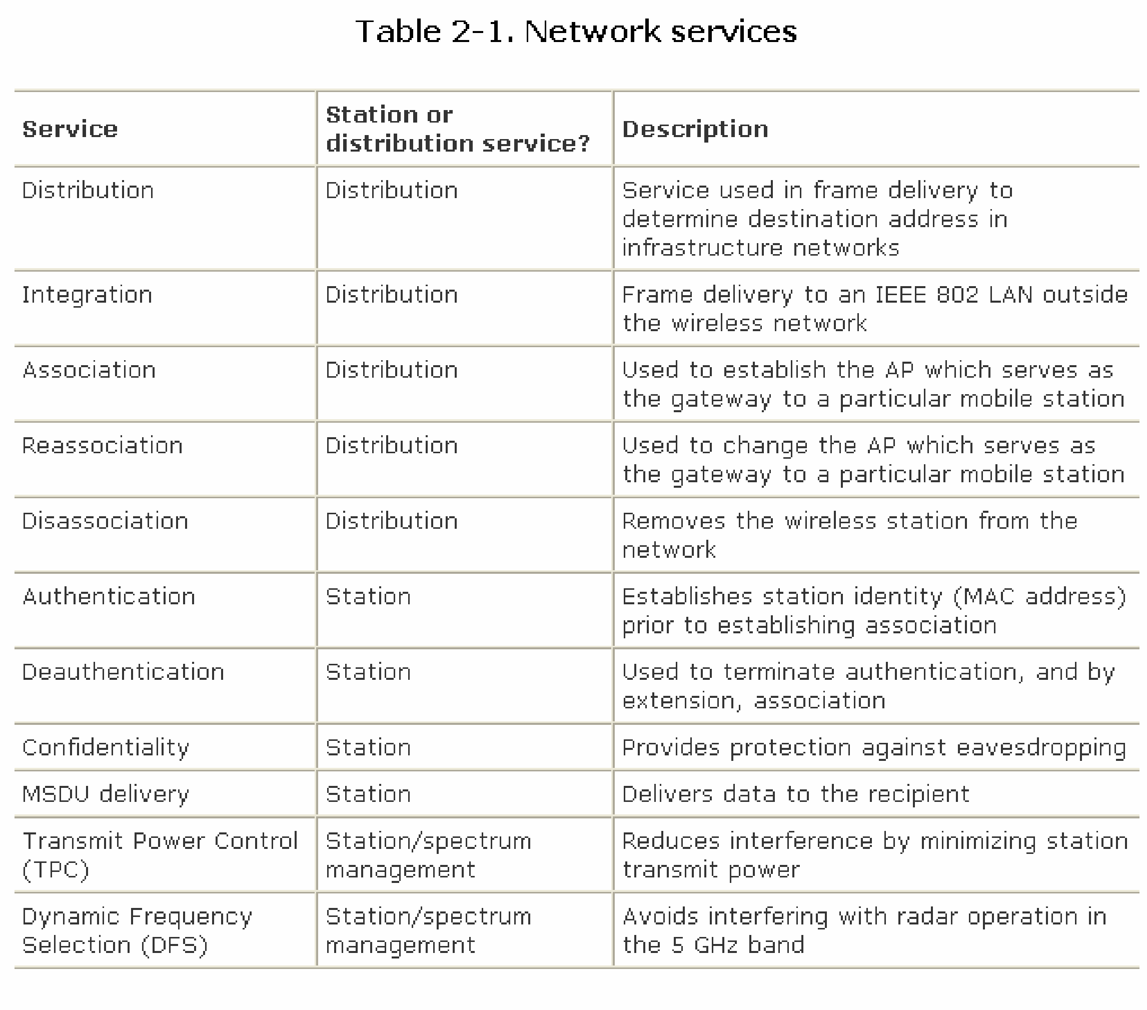


Table 2-1. Network services

Service	Station or distribution service?	Description
Distribution	Distribution	Service used in frame delivery to determine destination address in infrastructure networks
Integration	Distribution	Frame delivery to an IEEE 802 LAN outside the wireless network
Association	Distribution	Used to establish the AP which serves as the gateway to a particular mobile station
Reassociation	Distribution	Used to change the AP which serves as the gateway to a particular mobile station
Disassociation	Distribution	Removes the wireless station from the network
Authentication	Station	Establishes station identity (MAC address) prior to establishing association
Deauthentication	Station	Used to terminate authentication, and by extension, association
Confidentiality	Station	Provides protection against eavesdropping
MSDU delivery	Station	Delivers data to the recipient
Transmit Power Control (TPC)	Station/spectrum management	Reduces interference by minimizing station transmit power
Dynamic Frequency Selection (DFS)	Station/spectrum management	Avoids interfering with radar operation in the 5 GHz band

2.4.2 Station services

Station services are part of every 802.11-compliant station and must be incorporated by any product claiming 802.11 compliance. Station services are provided by both mobile stations and the wireless interface on access points. Stations provide frame delivery services to allow message delivery, and, in support of this task, they may need to use the authentication services to establish associations. Stations may also wish to take advantage of confidentiality functions to protect messages as they traverse the vulnerable wireless link.

2.4.3 Distribution system services

Distribution system services connect access points to the distribution system. The major role of access points is to extend the services on the wired network to the wireless network; this is done by providing the distribution and integration services to the wireless side. Managing mobile station associations is the other major role of the distribution system. To maintain association data and station location information, the distribution system provides the association, reassociation, and disassociation services.

2.4.4 Confidentiality and access control

Confidentiality and access control services are intertwined. In addition to secrecy of the data in transit, the confidentiality service also proves the integrity of frame contents. Both secrecy and integrity depend on shared cryptographic keying, so the confidentiality service necessarily depends on other services to provide authentication and key management.

Authentication and key management (AKM)

> Cryptographic integrity is worthless if it does not prevent unauthorized users from attaching to the network. The confidentiality service depends on the authentication and key management suite to establish user identity and encryption keys. Authentication may be accomplished through an external protocol, such as 802.1X, or with pre-shared keys.

Cryptographic algorithms

> Frames may be protected by the traditional WEP algorithm, using 40- or 104-bit secret keys, the Temporal Key Integrity Protocol (TKIP), or the Counter Mode CBC-MAC Protocol (CCMP).

Origin authenticity

> TKIP and CCMP allow the receiver to validate the sender's MAC address to prevent spoofing attacks. Origin authenticity protection is only available for unicast data.

Replay detection

TKIP and CCMP protect against replay attacks by incorporating a sequence counter that is validated upon receipt. Frames which are "too old" to be valid are discarded.

External protocols and systems

The confidentiality service depends heavily on external protocols to run. Key management is provided by 802.1X, which together with EAP carries authentication data. 802.11 places no constraint on the protocols used, but the most common choices are EAP for authentication, and RADIUS to interface with the authentication server.

2.4.5 Spectrum management services

Spectrum management services are a special subset of station services. They are designed to allow the wireless network to react to conditions and change radio settings dynamically. Two services were defined in 802.11h to help meet regulatory requirements.

The first service, transmit power control (TPC), can dynamically adjust the transmission power of a station. Access points will be able to use the TPC operations to advertise the maximum permissible power, and reject associations from clients that do not comply with the local radio regulations. Clients can use TPC to adjust power so that range is "just right" to get to the access point. Digital cellular systems have a similar feature designed to extend the battery life of mobile phones. Lower transmit power also will have some benefit in the form of increased battery life, though the extent of the improvement will depend on how much the transmit power can be reduced from what the client would otherwise have used.

The second service, dynamic frequency selection (DFS), was developed mainly to avoid interfering with some 5 GHz radar systems in use in Europe. Although originally developed to satisfy European regulators, the underlying principles have been required by other regulators as well. DFS was key to the U.S. decision to open up more spectrum in the 5 GHz band in 2004. DFS includes a way for the access point to quiet the channel so that it can search for radar without interference, but the most significant part of DFS is the way that it can reassign the channel on an access point on the fly. Clients are informed of the new channel just before the channel is switched.

2.5 Wireless Networking Standards

Institute of Electrical and Electronics Engineers (IEEE) has specified various WLAN standards. Some important standards are summarized below in Table 2.2:

Standards	Description	Status
802.11	Standard for WLAN operations at data rates up to 2 Mbps in the 2.4-GHz ISM band	Approved in July 1997
802.11a	Standard for WLAN operations at data rates up to 54 Mbps in the 5-GHz UNII band	Approved in Sept 1999. End-user products began hipping in early 2002
802.11b	Standard for WLAN operations at data rates up to 11 Mbps in the 2.4-GHz ISM band	Sept 1999. End-user products began shipping in early 2000
802.11g	High-rate extension to 802.11b allowing for data rates up to 54 Mbps in the 2.4-GHz ISM band	Draft standard adopted Nov 2001. Full ratification expected late 2002 or early 2003
802.11e	**Enhance the 802.11 MAC to improve and manage Quality of Service, provide classes of service, and enhanced security and authentication mechanisms. These enhancements should provide the quality required for services such as IP telephony and video streaming**	Still in development, i.e., in the task group (TG) stage
802.11f	Develop recommended practices for an Inter- access Point Protocol (IAPP) which provides the necessary capabilities to achieve multi-vendor AP interoperability across a DS supporting IEEE P802.11 Wireless LAN Links	Still in development, i.e., in the task group (TG) stage
802.11i	Enhance the 802.11 Medium Access Control (MAC) to enhance security and authentication mechanisms	Still in development, i.e., in the task group (TG) stage

Table 2.2 IEEE WLAN Standards

The purpose of IEEE 802.11i standard is to enhance the 802.11 MAC to enhance security and authentication mechanisms. It defines the encapsulation of EAP IEEE 802.11 WLAN

3 The 802.11 Basic Security Mechanisms

Basic wireless security is provided by the following built-in functions:

- SSIDs
- Wired Equivalent Privacy (WEP)
- Media Access Control (MAC) address verification

3.1 SSIDs:

An SSID is a code that identifies membership with a WAP. All wireless devices that want to communicate on a network must have their SSID set to the same value as the WAP SSID to establish connectivity with the WAP.

By default, a WAP broadcasts its SSID every few seconds. This broadcast can be stopped so that a drive-by hacker can't automatically discover the SSID and hence the WAP. However, because the SSID is included in the beacon of every wireless frame, it is easy for a hacker equipped with sniffing equipment to discover the value and fraudulently join the network.

Being able to join a wireless network by the mere fact of knowing the SSID is referred to as open authentication.

3.2 Wired Equivalent Privacy

WEP can be used to alleviate the problem of SSID broadcasts by encrypting the traffic between the wireless clients and WAPs. Joining a wireless network using WEP is referred to as shared-key authentication, where the WAP sends a challenge to the wireless client who must return it encrypted. If the WAP can decipher the client's response, the WAP has the proof that the client possesses valid keys and therefore has the right to join the wireless network. WEP comes in two encryption strengths: 64-bit and 128-bit.

However, WEP is not considered secure: A hacker sniffing first the challenge and then the encrypted response could reverse-engineer the process and deduce the keys used by the client and WAP.

3.3 MAC Address Verification

To further wireless security, a network administrator could use MAC address filtering, in which the WAP is configured with the MAC addresses of the wireless clients that are to be permitted access.

Unfortunately, this method is also not secure because frames could be sniffed to discover a valid MAC address, which the hacker could then spoof.

4 Security Principles

4.1 What Is Security?

The word security can mean different things when taken in different contexts. For instance, we talk about security in relation to national policy, personal safety, financial risk, and privacy of communication. We even use the word to describe our state of emotions. So what is the common thread that links these definitions? Why do we use the same word to describe protection from muggers and protection from hackers?

We propose to define security in the context of two groups: "the good guys" and the "bad guys." It doesn't matter if we are talking about people, robots, or computers; in our definition, if there are no "bad guys," you are secure by default. Imagine a perfect world with no crime—there would be no need for a police force. Security tries to create such a perfect world, not globally but in a controlled space; it tries to create a bubble within which there are no "bad guys" at a given time. National security performs this role for a country, personal security for the living space of an individual, and emotional security for the confines of a person's mind. If the security is implemented successfully, the entity being secured is immune from the influence of the "bad guys." It is as though the bad guys don't exist.

As we look at Wi-Fi security, keep this goal in mind: Make it as though the bad guys don't exist. It is dangerous to focus on only one mechanism of security, such as data encryption, or to concentrate on defending against a certain type of attack. Also, it is wrong to ignore security weaknesses just because they have low consequences. Suppose a virus succeeds in getting into your computer, but it does no damage. Would we say security hasn't been breached because no damage was done? No, because although there is no consequence, we still have a security breach. In the same way, solutions for Wi-Fi LAN security should prevent any sort of interference with, or monitoring of, your actions. This is the ultimate goal of security.

With the new Wi-Fi security measures , we can come close to this ultimate security goal. There is only one thing we cannot achieve because we are using wireless. Someone can prevent your communications by transmitting a jamming signal; in other words, the bad guys will still be able to demonstrate their presence by blocking communication. But if we design our security protocols correctly, and install them correctly, that is all they can do.

4.2 Good Security Thinking

Rather than dive straight into the methods for implementing network security, let's take a high-level look at six principles of security thinking. You won't find these principles in a book such as How to Make Friends and Influence People; they are inevitably based on a philosophy of mistrust.

1. Don't talk to anyone you don't know.
2. Accept nothing without a guarantee.
3. Treat everyone as an enemy until proved otherwise.
4. Don't trust your friends for long.
5. Use well-tried solutions.
6. Watch the ground you are standing on for cracks.

The sixth principle is a bit cryptic. The "ground" in this context refers to the pile of assumptions we all stand on. This sixth principle is the real danger zone in security and one of the most fruitful for the enemy.

5 802.11 Security Threats

5.1 Wireless Network Sniffing

Sniffing is eavesdropping on the network. A (packet) sniffer is a program that intercepts and decodes network traffic broadcast through a medium. Sniffing is the act by a machine S of making copies of a network packet sent by machine A intended to be received by machine B. Such sniffing, strictly speaking, is not a TCP/IP problem, but it is enabled by the choice of broadcast media, Ethernet and 802.11, as the physical and data link layers.

Sniffing has long been a reconnaissance technique used in wired networks. Attackers sniff the frames necessary to enable the exploits described in later sections. Sniffing is the underlying technique used in tools that monitor the health of a network. Sniffing can also help find the easy kill as in scanning for open access points that allow anyone to connect, or capturing the passwords used in a connection session that does not even use WEP, or in telnet, rlogin and ftp connections.

It is easier to sniff wireless networks than wired ones. It is easy to sniff the wireless traffic of a building by setting shop in a car parked in a lot as far away as a mile, or while driving around the block. In a wired network, the attacker must find a way to install a sniffer on one or more of the hosts in the targeted subnet. Depending on the equipment used in a LAN, a sniffer needs to be run either on the victim machine whose traffic is of interest or on some other host in the same subnet as the victim. An attacker at large on the Internet has other techniques that make it possible to install a sniffer remotely on the victim machine.

5.1.1 Passive Scanning

Scanning is the act of sniffing by tuning to various radio channels of the devices. A passive network scanner instructs the wireless card to listen to each channel for a few messages. This does not reveal the presence of the scanner.

An attacker can passively scan without transmitting at all. Several modes of a station permit this. There is a mode called RF monitor mode that allows every frame appearing on a channel to be copied as the radio of the station tunes to various channels. This is analogous to placing a wired Ethernet card in promiscuous mode. This mode is not enabled by default. Some wireless cards on the market today have disabled this feature in the default firmware. One can buy wireless cards whose firmware and corresponding driver software together permit reading of all raw 802.11 frames. A station in monitor mode can capture packets without associating with an AP or ad-hoc network. The so-called promiscuous mode allows the capture of all wireless packets of an associated network. In this mode, packets cannot be read until authentication and association are completed.

An example sniffer is Kismet (http://www.kismetwireless.net). An example wireless card that permits RF monitor modes is Cisco Aironet AIR-PCM342.

5.1.2 Detection of SSID

The attacker can discover the SSID of a network usually by passive scanning because the SSID occurs in the following frame types: Beacon, Probe Requests, Probe Responses, Association Requests, and Reassociation Requests. Recall that management frames are always in the clear, even when WEP is enabled.

On a number of APs, it is possible to configure so that the SSID transmitted in the Beacon frames is masked, or even turn off Beacons altogether. The SSID shown in the Beacon frames is set to null in the hope of making the WLAN invisible unless a client already knows the correct SSID. In such a case, a station wishing to join a WLAN begins the association process by sending Probe Requests since it could not detect any APs via Beacons that match its SSID.

If the Beacons are not turned off, and the SSID in them is not set to null, an attacker obtains the SSID included in the Beacon frame by passive scanning.

When the Beacon displays a null SSID, there are two possibilities. Eventually, an Associate Request may appear from a legitimate station that already has a correct SSID. To such a request, there will be an Associate Response frame from the AP. Both frames will contain the SSID in the clear, and the attacker sniffs these. If the station wishes to join any available AP, it sends Probe Requests on all channels, and listens for Probe Responses that contain the SSIDs of the APs. The station considers all Probe Responses, just as it would have with the non-empty SSID Beacon frames, to select an AP. Normal association then begins. The attacker waits to sniff these Probe Responses and extract the SSIDs.

If Beacon transmission is disabled, the attacker has two choices. The attacker can keep sniffing waiting for a voluntary Associate Request to appear from a legitimate station that already has a correct SSID and sniff the SSID as described above. The attacker can also chose to actively probe by injecting frames that he constructs, and then sniffs the response as described in a later section.

When the above methods fail, SSID discovery is done by active scanning .

5.1.3 Collecting the MAC Addresses

The attacker gathers legitimate MAC addresses for use later in constructing spoofed frames. The source and destination MAC addresses are always in the clear in all the frames. There are two reasons why an attacker would collect MAC addresses of stations and APs participating in a wireless network. (1) The attacker wishes to use these values in spoofed frames so that his station or AP is not identified. (2) The targeted AP may be controlling access by filtering out frames with MAC addresses that were not registered.

5.1.4 Collecting the Frames for Cracking WEP

The goal of an attacker is to discover the WEP shared-secret key. Often, the shared key can be discovered by guesswork based on a certain amount of social engineering regarding the administrator who configures the wireless LAN and all its users. Some client software stores the WEP keys in the operating system registry or initialization scripts. In the following, we assume that the attacker was unsuccessful in obtaining the key in this manner. The attacker then employs systematic procedures in cracking the WEP. For this purpose, a large number (millions) of frames need to be collected because of the way WEP works.

The wireless device generates on the fly an Initialization Vector (IV) of 24-bits. Adding these bits to the shared-secret key of either 40 or 104 bits, we often speak of 64-, or 128-bit encryption. WEP generates a pseudo-random key stream from the shared secret key and the IV. The CRC-32 checksum of the plain text, known as the Integrity Check (IC) field, is appended to the data to be sent. It is then exclusive-ORed with the pseudo-random key stream to produce the cipher text. The IV is appended in the clear to the cipher text and transmitted. The receiver extracts the IV, uses the secret key to re-generate the random key stream, and exclusive-ORs the received cipher text to yield the original plaintext.

Certain cards are so simplistic that they start their IV as 0 and increment it by 1 for each frame, resetting in between for some events. Even the better cards generate weak IVs from which the first few bytes of the shared key can be computed after statistical analyses. Some implementations generate fewer mathematically weak vectors than others do.

The attacker sniffs a large number of frames from a single BSS. These frames all use the same key. The mathematics behind the systematic computation of the secret shared key from a collection of cipher text extracted from these frames is described elsewhere in this volume. What is needed however is a collection of frames that were encrypted using “mathematically-weak” IVs. The number of encrypted frames that were mathematically weak is a small percentage of all frames. In a collection of a million frames, there may only be a hundred mathematically weak frames. It is conceivable that the collection may take a few hours to several days depending on how busy the WLAN is.

Given a sufficient number of mathematically weak frames, the systematic computation that exposes the bytes of the secret key is intensive. However, an attacker can employ powerful computers. On an average PC, this may take a few seconds to hours. The storage of the large numbers of frames is in the several hundred-mega bytes to a few giga bytes range.

An example of a WEP cracking tool is AirSnort (http://airsnort.shmoo.com).

5.1.5 Detection of the Sniffers

Detecting the presence of a wireless sniffer, who remains radio-silent, through network security measures is virtually impossible. Once the attacker begins probing (i.e., by injecting packets), the presence and the coordinates of the wireless device can be detected.

5.2 Wireless Spoofing

There are well-known attack techniques known as spoofing in both wired and wireless networks. The attacker constructs frames by filling selected fields that contain addresses or identifiers with legitimate looking but non-existent values, or with values that belong to others. The attacker would have collected these legitimate values through sniffing.

5.2.1 MAC Address Spoofing

The attacker generally desires to be hidden. But the probing activity injects frames that are observable by system administrators. The attacker fills the Sender MAC Address field of the injected frames with a spoofed value so that his equipment is not identified.

Typical APs control access by permitting only those stations with known MAC addresses. Either the attacker has to compromise a computer system that has a station, or he spoofs with legitimate MAC addresses in frames that he manufactures. MAC addresses are assigned at the time of manufacture, but setting the MAC address of a wireless card or AP to an arbitrary chosen value is a simple matter of invoking an appropriate software tool that engages in a dialog with the user and accepts values. Such tools are routinely included when a station or AP is purchased. The attacker, however, changes the MAC address programmatically, sends several frames with that address, and repeats this with another MAC address. In a period of a second, this can happen several thousand times.

When an AP is not filtering MAC addresses, there is no need for the attacker to use legitimate MAC addresses. However, in certain attacks, the attacker needs to have a large number of MAC addresses than he could collect by sniffing. Random MAC addresses are generated. However, not every random sequence of six bytes is a MAC address. The IEEE assigns globally the first three bytes, and the manufacturer chooses the last three bytes. The officially assigned numbers are publicly available. The attacker generates a random MAC address by selecting an IEEE-assigned three bytes appended with an additional three random bytes.

5.2.2 IP spoofing

Replacing the true IP address of the sender (or, in rare cases, the destination) with a different address is known as IP spoofing. This is a necessary operation in many attacks.

The IP layer of the OS simply trusts that the source address, as it appears in an IP packet is valid. It assumes that the packet it received indeed was sent by the host officially assigned that source address. Because the IP layer of the OS normally adds these IP addresses to a data packet, a spoofer must circumvent the IP layer and talk directly to the raw network device. Note that the attacker's machine cannot simply be assigned the IP address of another host X using ifconfig or a similar configuration tool. Other hosts, as well as X, will discover (through ARP, for example) that there are two machines with the same IP address.

IP spoofing is an integral part of many attacks. For example, an attacker can silence a host A from sending further packets to B by sending a spoofed packet announcing a window size of zero to A as though it originated from B.

5.2.3 Frame Spoofing

The attacker will inject frames that are valid by 802.11 specifications, but whose content is carefully spoofed as described above.

Frames themselves are not authenticated in 802.11 networks. So when a frame has a spoofed source address, it cannot be detected unless the address is wholly bogus. If the frame to be spoofed is a management or control frame, there is no encryption to deal with. If it is a data frame, perhaps as part of an on-going MITM attack, the data payload must be properly encrypted.

Construction of the byte stream that constitutes a spoofed frame is a programming matter once the attacker has gathered the needed information through sniffing and probing. There are software libraries that ease this task. Examples of such libraries are libpcap (sourceforge.net/projects/libpcap/), libnet (libnet.sourceforge.net/), libdnet (libdnet. sourceforge.net/) and libradiate (www.packetfactory.net/projects/libradiate/).

The difficulty here is not in the construction of the contents of the frame, but in getting, it radiated (transmitted) by the station or an AP. This requires control over the firmware and driver of the wireless card that may sanitize certain fields of a frame. Therefore, the attacker selects his equipment carefully. Currently, there are off-the-shelf wireless cards that can be manipulated. In addition, the construction of special purpose wireless cards is within the reach of a resourceful attacker.

5.3 Wireless Network Probing

Even though the attacker gathers considerable amount of information regarding a wireless network through sniffing, without revealing his wireless presence at all, there are pieces that may still be missing. The attacker then sends artificially constructed packets to a target that trigger useful responses. This activity is known as probing or active scanning.

The target may discover that it is being probed, it might even be a honey pot (www.honeynet.org/) target carefully constructed to trap the attacker. The attacker would try to minimize this risk.

5.3.1 Detection of SSID

Detection of SSID is often possible by simply sniffing Beacon frames as describe in a previous section.

If Beacon transmission is disabled, and the attacker does not wish to patiently wait for a voluntary Associate Request to appear from a legitimate station that already has a correct SSID, or Probe Requests from legitimate stations, he will resort to probing by injecting a Probe Request frame that contains a spoofed source MAC address. The Probe Response frame from the APs will contain, in the clear, the SSID and other information similar to that in the Beacon frames were they enabled. The attacker sniffs these Probe Responses and extracts the SSIDs.

Some models of APs have an option to disable responding to Probe Requests that do not contain the correct SSID. In this case, the attacker determines a station associated with the AP, and sends the station a forged Disassociation frame where the source MAC address is set to that of the AP. The station will send a Reassociation Request that exposes the SSID.

5.3.2 Detection of APs and stations

Every AP is a station, so SSIDs, MAC addresses are gathered as described above.

Certain bits in the frames identify that the frame is from an AP. If we assume that WEP is either disabled or cracked, the attacker can also gather the IP addresses of the AP and the stations.

5.3.3 Detection of Probing

Detection of probing is possible. The frames that an attacker injects can also be heard by the intrusion detection systems (IDS) of hardened wireless LAN. There is GPS-enabled equipment that can identify the physical coordinates of a wireless device through which the probe frames are being transmitted.

5.4. AP Weaknesses

APs have weaknesses that are both due to design mistakes and user interfaces that promote weak passwords, etc. It has been demonstrated by many publicly conducted war-driving efforts (www.worldwidewardrive.org) in major cities around the world that a large majority of the deployed APs are poorly configured, most with WEP disabled, and configuration defaults, as set up the manufacturer, untouched.

5.4.1 Configuration

The default WEP keys used are often too trivial. Different APs use different techniques to convert the user's key board input into a bit vector. Usually 5 or 13 ASCII printable characters are directly mapped by concatenating their ASCII 8-bit codes into a 40-bit or 104-bit WEP key. A stronger key can be constructed from an input of 26 hexadecimal digits. It is possible to form an even stronger104 bit WEP key by truncating the MD5 hash of an arbitrary length pass phrase.

5.4.2 Defeating MAC Filtering

Typical APs permit access to only those stations with known MAC addresses. This is easily defeated by the attacker who spoofs his frames with a MAC address that is registered with the AP from among the ones that he collected through sniffing. That a MAC address is registered can be detected by observing the frames from the AP to the stations.

5.4.3 Rogue AP

Access points that are installed without proper authorization and verification that overall security policy is obeyed are called rogue APs. These are installed and used by valid users. Such APs are configured poorly, and attackers will find them.

5.4.4 Trojan AP

An attacker sets up an AP so that the targeted station receives a stronger signal from it than what it receives from a legitimate AP. If WEP is enabled, the attacker would have already cracked it. A legitimate user selects the Trojan AP because of the stronger signal, authenticates and associates. The Trojan AP is connected to a system that collects the IP traffic for later analyses. It then transmits all the frames to a legitimate AP so that the victim user does not recognize the on-going MITM attack. The attacker can steal the users password, network access, compromise the user's system to give himself root access. This attack is called the Evil Twin Attack.

It is easy to build a Trojan AP because an AP is a computer system optimized for its intended application. A general purpose PC with a wireless card can be turned into a capable AP. An example of such software is HostAP (http://hostap.epitest.fi/). Such a Trojaned AP would be formidable.

5.4.5 Equipment Flaws

A search on www.securityfocus.com with "access point vulnerabilities" will show that numerous flaws in equipment from well-known manufacturers are known. For example, one such AP crashes when a frame is sent to it that has the spoofed source MAC address of itself. Another AP features an embedded TFTP (Trivial File Transfer Protocol) server. By requesting a file named config.img via TFTP, an attacker receives the binary image of the AP configuration. The image includes the administrator's password required by the HTTP user interface, the WEP encryption keys, MAC address, and SSID. Yet another AP returns the WEP keys, MAC filter list, administrator's password when sent a UDP packet to port 27155 containing the string "gstsearch".

It is not clear how these flaws were discovered. The following is a likely procedure. Most manufacturers design their equipment so that its firmware can be flashed with a new and improved one in the field. The firmware images are downloaded from the manufacturers' web site. The CPU used in the APs can be easily recognized, and the firmware can be systematically disassembled revealing the flaws at the assembly language level.

Comprehensive lists of such equipment flaws are likely circulating among the attackers.

5.5. Denial of Service

A denial of service (DoS) occurs when a system is not providing services to authorized clients because of resource exhaustion by unauthorized clients. In wireless networks, DoS attacks are difficult to prevent, difficult to stop an on-going attack and the victim and its clients may not even detect the attacks. The duration of such DoS may range from milliseconds to hours. A DoS attack against an individual station enables session hijacking.

5.5.1 Jamming the Air Waves

A number of consumer appliances such as microwave ovens, baby monitors, and cordless phones operate on the unregulated 2.4GHz radio frequency. An attacker can unleash large amounts of noise using these devices and jam the airwaves so that the signal to noise drops so low, that the wireless LAN ceases to function. The only solution to this is RF proofing the surrounding environment.

5.5.2 Flooding with Associations

The AP inserts the data supplied by the station in the Association Request into a table called the association table that the AP maintains in its memory. The IEEE 802.11 specifies a maximum value of 2007 concurrent associations to an AP. The actual size of this table varies among different models of APs. When this table overflows, the AP would refuse further clients.

Having cracked WEP, an attacker authenticates several non-existing stations using legitimate-looking but randomly generated MAC addresses. The attacker then sends a flood of spoofed associate requests so that the association table overflows.

Enabling MAC filtering in the AP will prevent this attack.

5.5.3 Forged Dissociation

The attacker sends a spoofed Disassociation frame where the source MAC address is set to that of the AP. The station is still authenticated but needs only to reassociate and sends Reassociation Requests to the AP. The AP may send a Reassociation Response accepting the station and the station can then resume sending data. To prevent Reassociation, the attacker continues to send Disassociation frames for a desired period.

5.5.4 Forged De-authentication

The attacker monitors all raw frames collecting the source and destination MAC addresses to verify that they are among the targeted victims. When a data or Association Response frame is observed, the attacker sends a spoofed Deauthentication frame where the source MAC address is spoofed to that of the AP. The station is now unassociated and unauthenticated, and needs to reconnect. To prevent a reconnection, the attacker continues to send Deauthentication frames for a desired period. The attacker may even rate limit the Deauthentication frames to avoid overloading an already congested network.

The mischievous packets of Disassociation and Deauthentication are sent directly to the client, so these will not be logged by the AP or IDS, and neither MAC filtering nor WEP protection will prevent it.

5.5.5 Power Saving

Power conservation is important for typical station laptops, so they frequently enter an 802.11 state called Doze. An attacker can steal packets intended for a station while the station is in the Doze state.

The 802.11 protocol requires a station to inform the AP through a successful frame exchange that it wishes to enter the Doze state from the Active state.

Periodically the station awakens and sends a PS-Poll frame to the AP. The AP will transmit in response the packets that were buffered for the station while it was dozing. This polling frame can be spoofed by an attacker causing the AP to send the collected packets and flush its internal buffers. An attacker can repeat these polling messages so that when the legitimate station periodically awakens and polls, AP will inform that there are no pending packets.

5.6 Man-in-the-Middle Attacks

Man-in-the-middle (MITM) attack refers to the situation where an attacker on host X inserts X between all communications between hosts B and C, and neither B nor C is aware of the presence of X. All messages sent by B do reach C but via X, and vice versa. The attacker can merely observe the communication or modify it before sending it out. An MITM attack can break connections that are otherwise secure. At the TCP level, SSH and VPN, e.g., are prone to this attack.

5.6.1 Wireless MITM

Assume that station B was authenticated with C, a legitimate AP. Attacker X is a laptop with two wireless cards. Through one card, he will present X as an AP. Attacker X sends Deauthentication frames to B using the C's MAC address as the source, and the BSSID he has collected. B gets deauthenticated and begins a scan for an AP and may find X on a channel different from C. There is a race condition between X and C. If B associates with X, the MITM attack succeeded. X will re-transmit the frames it receives from B to C, and the frames it receives from C to B after suitable modifications.

The package of tools called AirJack (http://802.11ninja.net/airjack/) includes a program called monkey_jack that automates the MITM attack. This is programmed well so that the odds of it winning in the race condition mentioned above are improved.

5.6.2 ARP Poisoning

ARP cache poisoning is an old problem in wired networks. Wired networks have deployed mitigating techniques. But, the ARP poisoning technique is re-enabled in the presence of APs that are connected to a switch/hub along with other wired clients.

ARP is used to determine the MAC address of a device whose IP address is known. The translation is performed with a table look-up. The ARP cache accumulates as the host continues to network. If the ARP cache does not have an entry for an IP address, the outgoing IP packet is queued, and an ARP Request packet that effectively requests "If your IP address matches this target IP address, then please let me know what your Ethernet address is" is broadcast. The host with the target IP is expected to respond with an ARP Reply, which contains the MAC address of the host. Once the table is updated because of receiving this response, all the queued IP packets can now be sent. The entries in the table expire after a set time in order to account for possible hardware address changes for the same IP address. This change may have happened, e.g., due to the NIC being replaced.

Unfortunately, the ARP does not provide for any verification that the responses are from valid hosts or that it is receiving a spurious response as if it has sent an ARP Request. ARP poisoning is an attack technique exploiting this lack of verification. It corrupts the ARP cache that the OS maintains with wrong MAC addresses for some IP addresses. An attacker accomplishes this by sending an ARP Reply packet that is deliberately constructed with a “wrong” MAC address. The ARP is a stateless protocol. Thus, a machine receiving an ARP Reply cannot determine if the response is due to a request it sent or not.

ARP poisoning is one of the techniques that enables the man-in-the-middle attack. An attacker on machine X inserts himself between two hosts B and C by (i) poisoning B so that C’s IP address is associated with X’s MAC address, (ii) poisoning C so that B’s address is associated with X’s MAC address, and (iii) relaying the packets X receives.

The ARP poison attack is applicable to all hosts in a subnet. Most APs act as transparent MAC layer bridges, and so all stations associated with it are vulnerable. If an access point is connected directly to a hub or a switch without an intervening router/firewall, then all hosts connected to that hub or switch are susceptible also. Note that recent devices aimed at the home consumer market combine a network switch with may be four or five ports, an AP, a router and a DSL/cable modem connecting to the Internet at large. Internally, the AP is connected to the switch. As a result, an attacker on a wireless station can become a MITM between two wired hosts, one wired one wireless, or both wireless hosts.

The tool called Ettercap ((http://ettercap.sourceforge.net) is capable of performing ARP poisoning.

5.6.3 Session Hijacking

Session hijacking occurs in the context of a “user”, whether human or computer. The user has an on-going connection with a server. Hijacking is said to occur when an attacker causes the user to lose his connection, and the attacker assumes his identity and privileges for a period.

An attacker disables temporarily the user’s system, say by a DoS attack or a buffer overflow exploit. The attacker then takes the identity of the user. The attacker now has all the access that the user has. When he is done, he stops the DoS attack, and lets the user resume. The user may not detect the interruption if the disruption lasts no more than a couple of seconds. Such hijacking can be achieved by using forged Disassociation DoS attack.

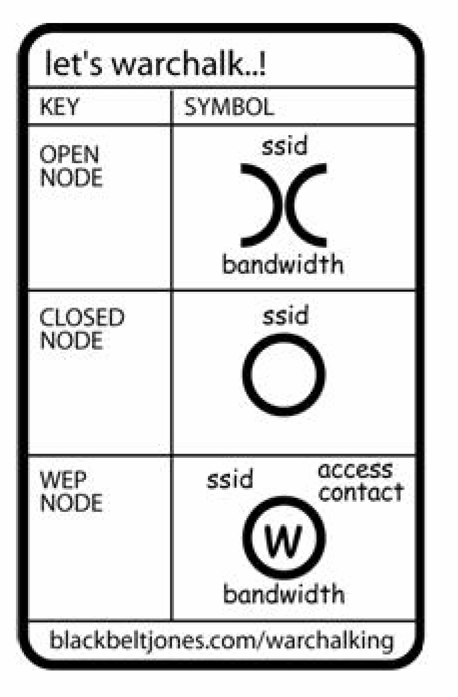
Corporate wireless networks are often set up so that the user is directed to an authentication server when his station attempts a connection with an AP. After the authentication, the attacker employs the session hijacking described above using spoofed MAC addresses.

5.7 War Driving

Equipped with wireless devices and related tools, and driving around in a vehicle or parking at interesting places with a goal of discovering easy-to-get-into wireless networks is known as war driving. War-drivers (http://www.wardrive.net/) define war driving as "The benign act of locating and logging wireless access points while in motion." This benign act is of course useful to the attackers.

5.7.1 War chalking

War chalking is the practice of marking sidewalks and walls with special symbols to indicate that wireless access is nearby so that others do not need to go through the trouble of the same discovery. A search on www.google.com with key words "war driving maps" will produce a large number of hits. Yahoo! Maps can show "Wi-fi Hotspots" near an address you give.



let's warchalk..!

KEY	SYMBOL
OPEN NODE	ssid bandwidth
CLOSED NODE	ssid
WEP NODE	ssid access contact W bandwidth

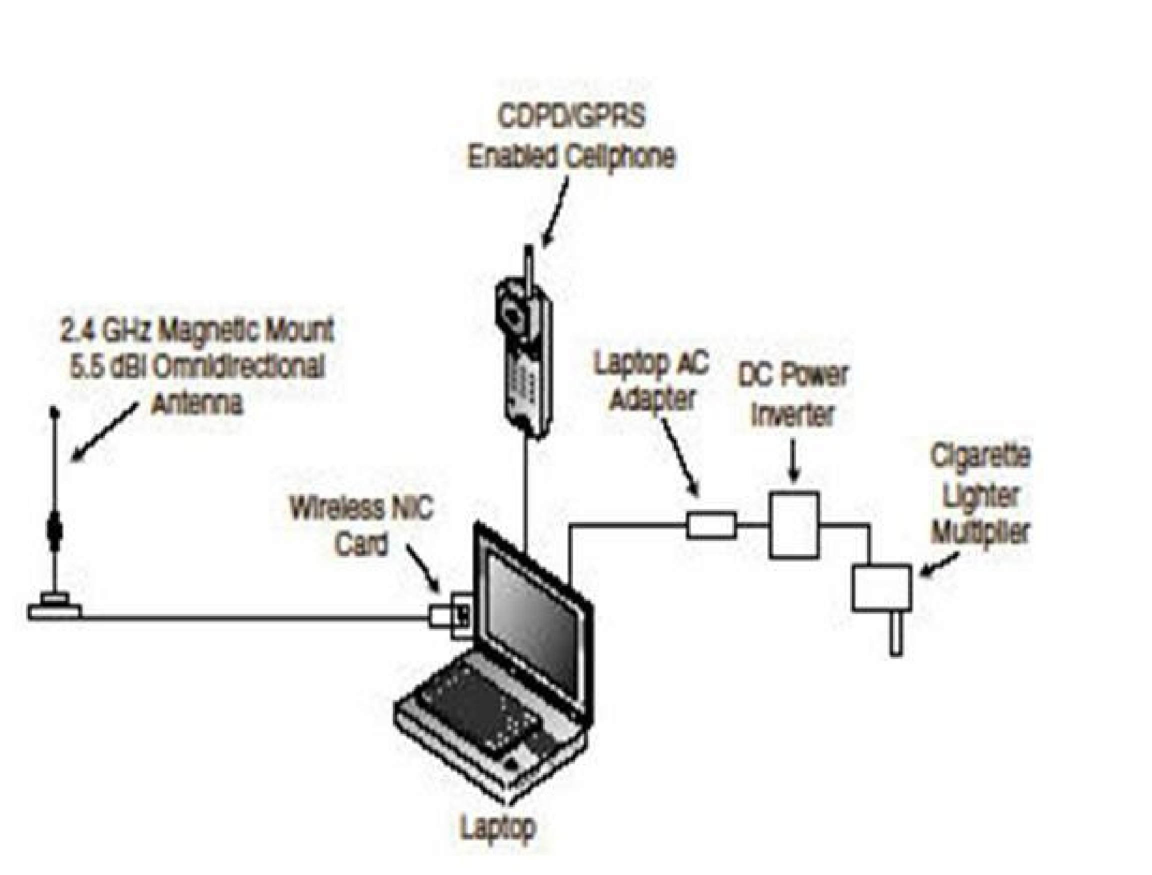
blackbeltjones.com/warchalking

5.7.2 Typical Equipment

The typical war driving equipment consists of a laptop computer system or a PDA with a wireless card, a GPS, and a high-gain antenna. Typical choice of an operating system is Linux or FreeBSD where open source sniffers (e.g., Kismet) and WEP crackers (e.g., AirSnort) are available. Similar tools (e.g., NetStumbler) that run on Windows are available.

War drivers need to be within the range of an AP or station located on the target network. The range depends on the transmit output power of the AP and the card, and the gain of the antenna. Ordinary access point antennae transmit their signals in all directions.

Often, these signals reach beyond the physical boundaries of the intended work area, perhaps to adjacent buildings, floors, and parking lots. With the typical 30mW wireless cards intended for laptops, the range is about 300 feet, but there are in 2004 wireless cards for laptops on the market that have 200mW. Directional high-gain antennae and an RF-amplifier can dramatically extend the range.


CDPD/GPRS Enabled Cellphone
2.4 GHz Magnetic Mount 5.5 dBI Omnidirectional Antenna
Laptop AC Adapter
DC Power Inverter
Cigarette Lighter Multiplier
Wireless NIC Card
Laptop

6. Securing the WLAN

There are many options available to help you secure your WLAN. The following is a brief list of some of these options. This chapter will discuss them in more detail.

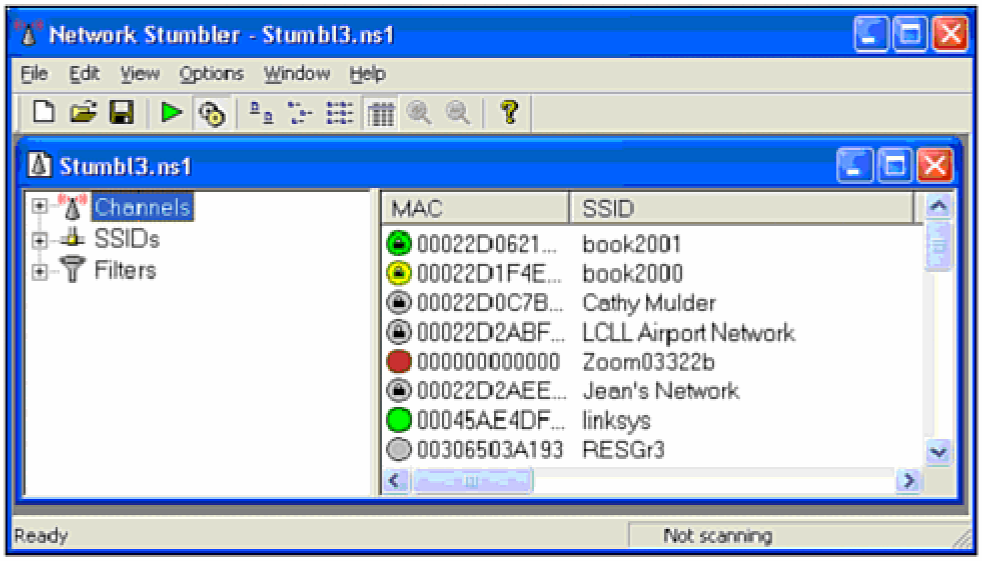
- WEP
- AP MAC filtering/broadcasting
- Antenna Radiation Zone
- DMZ
- Firewalls
- VPNs
- RADIUS
- TKIP
- AES
- SSL (Authentication Privacy)
- IDSs

6.1 Access Point-Based Security Measures

For WLANs, the first step in security hardening is to focus on the access point. Since the AP is the foundation of wireless LAN data transfer, you must ensure that it is part of the solution, instead of the problem.

6.1.1 WEP

It is true that the current version of WEP is crackable. However, most of the people who would attempt to access your wireless network will not want to put forth the effort required to crack WEP. The curious hacker will see that your network is using WEP and bypass it for an open network next door. The script kiddie will also bypass the WEP-protected WLAN because she will not have the patience or the aptitude to successfully penetrate the protection. Using a popular program such as NetStumbler, a hacker can easily spot the WEP-protected networks as well as your neighbor's open one. Which network do you think would be the victim


Network Stumbler - Stumbl3.ns1
File Edit View Options Window Help
Stumbl3.ns1
Channels
SSIDs
Filters
Ready
Not scanning

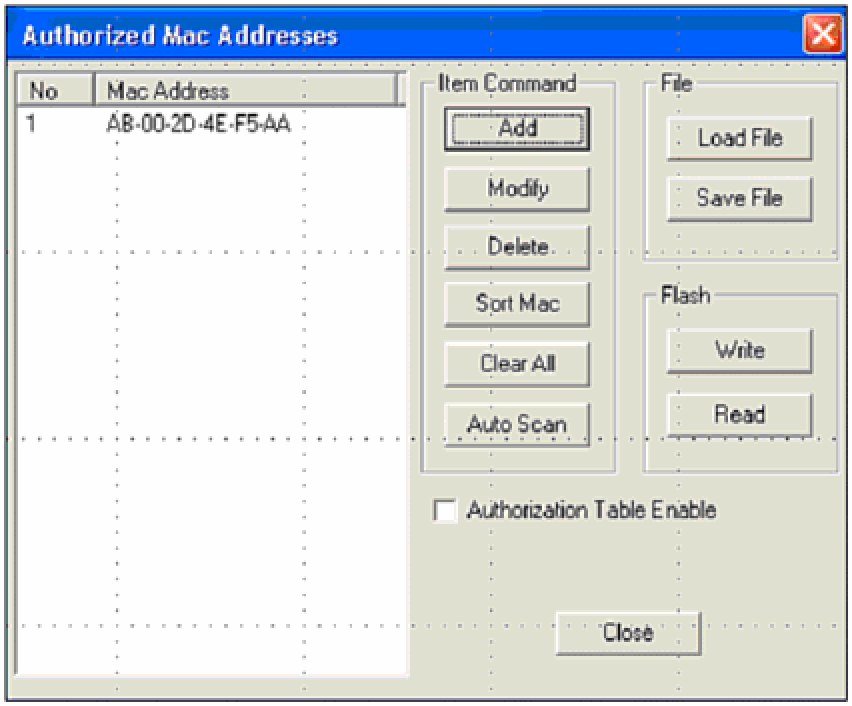
MAC	SSID
00022D0621...	book2001
00022D1F4E...	book2000
00022D0C7B...	Cathy Mulder
00022D2ABF...	LCLL Airport Network
000000000000	Zoom03322b
00022D2AEE...	Jean's Network
00045AE4DF...	linksys
00306503A193	RESGr3

Fig- 6.1 NetStumbler showing user WEP-protected and unprotected WLANs.

In other words, by enabling a protection that is minimally effective, you can eliminate 99% of your threat. Similar to a car lock, WEP will protect your network from passers-by; however, just as a dedicated thief will quickly bypass the lock by smashing a car window, a dedicated hacker will put forth the effort to crack WEP if it is the only thing between him and your network.

6.1.2 MAC Filtering

Every device on a wireless network, by default, has a unique address that's used to identify one WNIC from another. This address is called the MAC address, which stands for Media Access Control. In theory, because every WNIC has been pre-assigned a 100% unique MAC address by the hardware vendor, an access point can be set up to only allow a preselected list of WNICs to connect. For example, the Linksys WAP11 includes a MAC filtering option in its software that will enable an administrator to define who can connect to the WLAN by listing all the allowed MAC addresses



No	Mac Address
1	AB-00-2D-4E-F5-AA

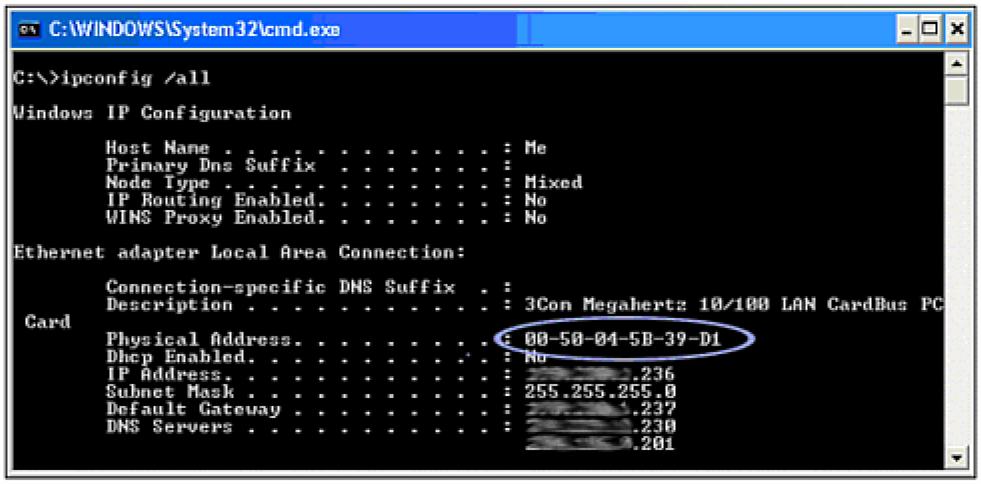
☐ Authorization Table Enable

Fig-6.2 MAC filtering in WAP11.

As you can see, this is fairly straightforward. To determine the MAC address of a network card, a user only has to go to Start Run and perform the steps in the following sections, depending on the operating system.

To determine the MAC address of a network card in Windows NT/2000/XP/.NET, follow these steps:

1. Type `cmd` .
2. In the command window, type `ipconfig /all` .
3. This will list the installed NICs. The MAC address is listed as the Physical Address



```
C:\>ipconfig /all

Windows IP Configuration

        Host Name . . . . . . . . . . . . : Me
        Primary Dns Suffix  . . . . . . . :
        Node Type . . . . . . . . . . . . : Mixed
        IP Routing Enabled. . . . . . . . : No
        WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : 3Com Megahertz 10/100 LAN CardBus PC
 Card
        Physical Address. . . . . . . . . : 00-50-04-5B-39-D1
        Dhcp Enabled. . . . . . . . . . . : No
        IP Address. . . . . . . . . . . . : [redacted].236
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : [redacted].237
        DNS Servers . . . . . . . . . . . : [redacted].230
                                            [redacted].201
```

Fig -6.3 Using IPCONFIG/ALL to obtain a MAC address.

Once you have the MAC addresses of all the connecting WNICs, you can set up the MAC filtering and enable it accordingly. This will stop any connection attempts made by unauthorized addresses.

6.1.3 Controlling the Radiation Zone

When a wireless network is active, it broadcasts radio frequency (RF) signals. These signals are used to transmit the wireless data from an access point to the WNIC and back again. The same signal is also used in ad-hoc networks, or even between PDAs with 802.11 WNICs. Although this particular use of RF technology is relatively new, the use of the radio wave is very old. In fact, one of the closest relatives to the wireless network is the wireless phone. Ironically, some wireless phones have started to incorporate the 2.4GHz range, which is the same frequency used by 802.11b WLANs.

When using a radio wave, there is a range limit imposed by the signal. Because of interference from various obstacles, including sunlight and air, the signals weaken the farther one travels from the broadcasting unit. If you could see these signals, you might see a circular, deteriorating globe that is strongest at the center. This virtual globe is known as the radiation zone.

What many people do not realize is that the radiation zone can be quite large, depending on the location and strength of the base unit. Although solid walls, metal beams, and electrical wiring can impede the signal, these zones are often much larger than advertised on the WLAN's documentation.

To illustrate this, you can perform a simple test using a wireless phone. Place your phone base near an open window and call someone you know. Then start walking. You might find that you can walk several hundred yards down the street and still maintain a relatively clear connection. In fact, depending on weather, hanging wires, and the strength of your phone's antenna, you could travel up to twice the distance advertised by the phone's documentation. This applies to your WLAN as well

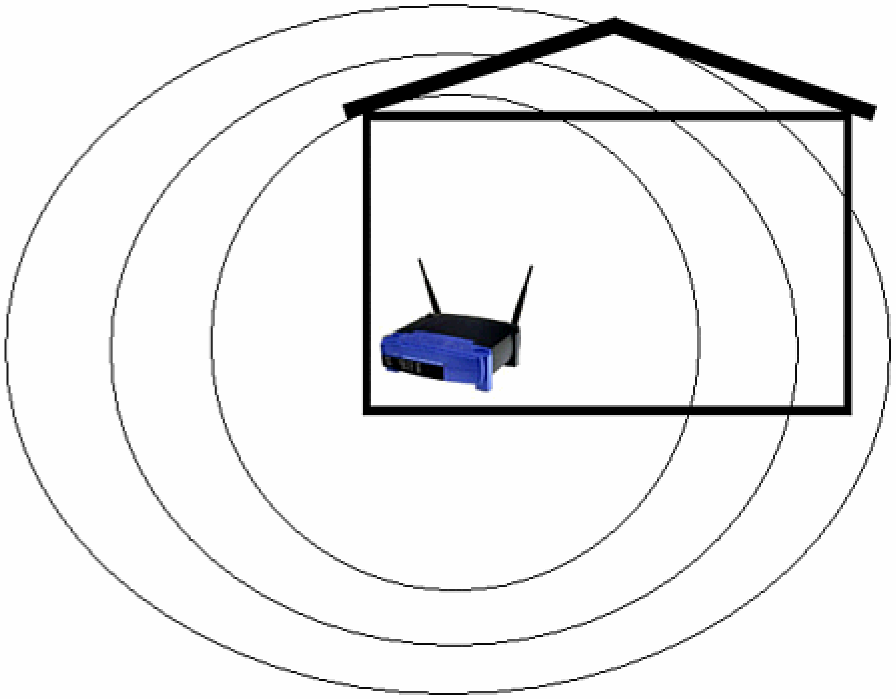


Fig – 6.4 WLAN leakage due to a fully powered access point located at the side of a building.

In addition to the fact that a radiation zone might extend far beyond an office's or home's physical boundaries, the tools and technology used by hackers can amplify the signal. Using a positional antenna, "Wireless Hardware," a hacker can narrow the window of detection and pick up signals from farther away. These same antennas are used to legitimately "push" wireless signals up to 20 miles or more. In other words, you will not be able to look out your window and see this hacker; he will probably be several blocks away. As a bonus for the hacker, the wireless signals have a tendency to bounce around in metropolitan areas, which means that even an unamplified signal can be detected several blocks in any direction.

Fortunately, there are several methods with which you can control this signal bleeding. The first method is to place the access point in a central location in your office. Although this might be obvious, many access points are set up on an outside room next to a wall, and worse, near a window. If there is a need to install several access points across a large space, try to position them as close to the center of the building, or as far away from outside walls, as possible. For example, in our house example, a simple movement of the access point has an obvious impact on the leakage of the wireless signals

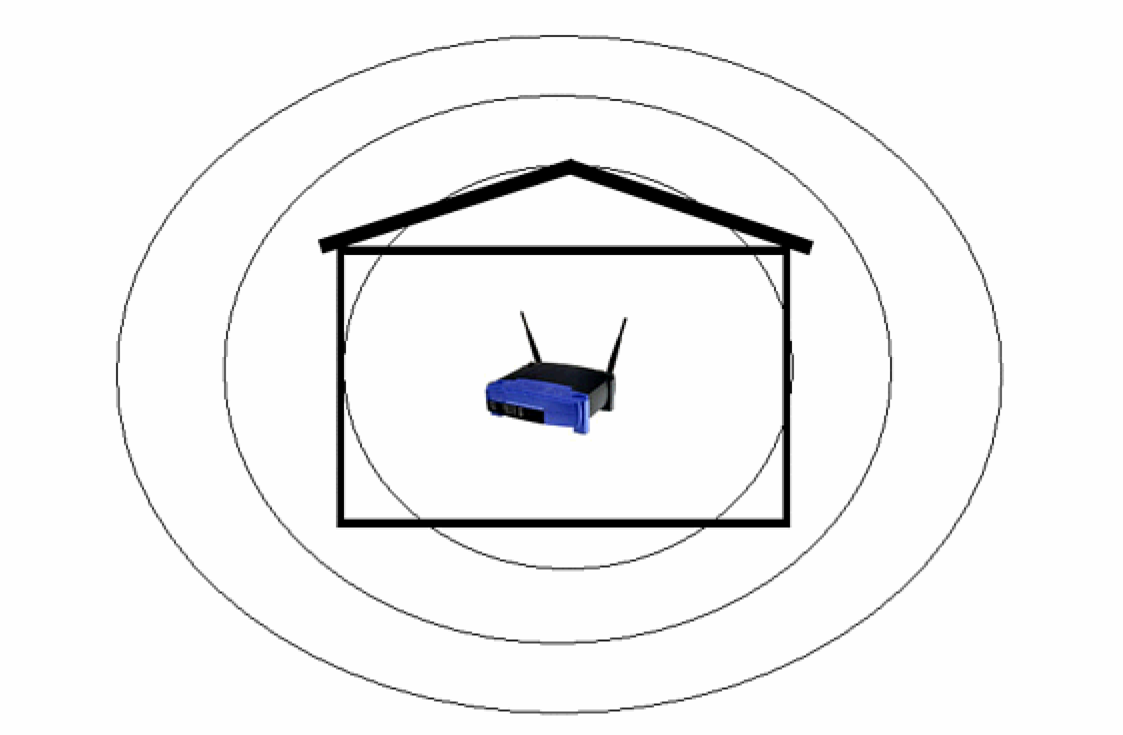
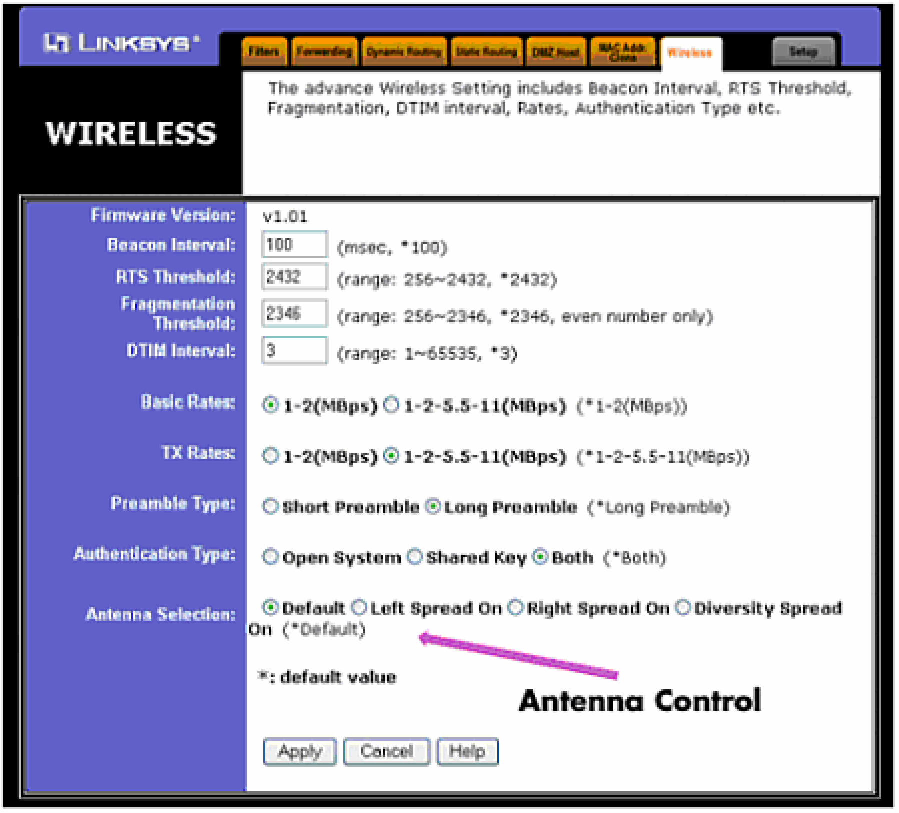


Fig - 6.5 WLAN bleed reduced because of central positioning.

In addition to managing the physical position of the access point, you can also control the signal sent out from the access point. In particular, you can control the power of the signal, which determines how far the signal travels. You can also control the direction of the signal by positioning the antenna and disabling one antenna to cut off one side of the access point. For example, in the Linksys BEFW1154, you can completely turn off the signal on either the right or left antenna This option is very handy in eliminating interference between access points and in restricting unneeded signals



WIRELESS

The advance Wireless Setting includes Beacon Interval, RTS Threshold, Fragmentation, DTIM interval, Rates, Authentication Type etc.

Firmware Version: v1.01

Beacon Interval: 100 (msec, *100)

RTS Threshold: 2432 (range: 256~2432, *2432)

Fragmentation Threshold: 2346 (range: 256~2346, *2346, even number only)

DTIM Interval: 3 (range: 1~65535, *3)

Basic Rates: ● 1-2(MBps) ○ 1-2-5.5-11(MBps) (*1-2(MBps))

TX Rates: ○ 1-2(MBps) ● 1-2-5.5-11(MBps) (*1-2-5.5-11(MBps))

Preamble Type: ○ Short Preamble ● Long Preamble (*Long Preamble)

Authentication Type: ○ Open System ○ Shared Key ● Both (*Both)

Antenna Selection: ● Default ○ Left Spread On ○ Right Spread On ○ Diversity Spread On (*Default)

*: default value

Antenna Control

Fig - 6.6 Antenna control.

Although this particular access point does not have the power option, such a feature comes with a few higher end models. If you are only going to use the access point in a small conference room, you do not need a high-powered, top-of-the-line access point. A low-budget model will suffice.

By using antenna management techniques, you can control the range of your WLAN. In high-rise buildings or apartment complexes, this can be a serious issue. Interference—and nosy neighbors—can quickly become a problem. By removing one antenna, reducing the output, and adjusting the position of the antenna, you can effectively keep the signal within a tight range

Fig – 6.7 Minimized leakage inside a residence.

Regardless of how much you control the radiation zone, there is a high chance that it will bleed slightly. In other words, this method of protection should be used in conjunction with other methods to completely secure the WLAN.

6.1.4 Defensive Security Through a DMZ

A DMZ, or demilitarized zone, is a concept of protection. A DMZ typically defines where you place servers that access the Internet. In other words, a Web server or mail server is often set up in a DMZ. This allows any Internet user to access the allocated resources on the server, but if the server becomes compromised, a hacker will not be able to use the "owned" computer to search out the rest of the network. Technically, a DMZ is actually its own little network, separate from the internal network, and separate from the Internet.

A firewall will often protect the DMZ from external threats. However, because the server must communicate to the outside world, the firewall will be configured to ignore many types of connections. In addition to isolating the servers, the DMZ is often set up to be easily accessible to internal network users. This is accomplished by the firewall hardware and software, which usually comes with a port set aside just for such a DMZ. For example, NetScreen has three ports: one for the Internet connection, the second for the internal connection, and the third for a DMZ into which a hub or switch can be connected to allow multiple servers.

This same port could be used to connect an access point, which is really nothing more than a wireless hub/switch. By doing this, you are basically placing the WLAN in a semi-trusted zone that is expected to be attacked by hackers. By operating with the mentality that your WLAN could already be owned, you can more appropriately plan who and what you allow to access the internal network. However, while this type of protection can help protect internal resources, it will not protect the wireless network users. Therefore, the DMZ should be just one part of your wireless security plan.

6.2 Third-Party Security Methods

While using the previously discussed security measures would help to lock down a WLAN, the simple fact is that this is not enough for security conscious environments where privacy is paramount. For situations like this, additional hardware and/or software can be implemented via third-party products. By integrating these products with existing technologies, your WLAN can become practically impenetrable.

6.2.1 Firewalls

If you read the last segment about using a DMZ to indirectly secure the WLAN, you will understand the importance of using a firewall. In short, a WLAN should be considered insecure and part of the public Internet. Thus, if you design your wireless network with this in mind, you should use a firewall to separate the wireless users from the internal users.

A firewall can do much to eliminate security threats. Depending on how it is set up and what types of policies are used, a firewall can effectively block all incoming requests that are not authorized. This creates a physical barrier to crackers who might have control over the wireless network and are trying to breach the internal network.

When it comes to selecting a firewall for the wireless part of your LAN, the best option is to use a dedicated hardware firewall, or simply to use one of the main firewalls protecting your existing Internet connection. Because the access point should exist off a DMZ, it can simply be connected to the DMZ port on any larger firewall appliance.

With this in mind, it is important to correctly set up security policies on the firewall. One of the most common problems with complex equipment is the increased chance of misconfiguration. The reason why we suggest using a dedicated firewall is because you can configure it to block everything, and then you can slowly relax these settings. Although this is possible with the main corporate Internet firewall, it is the less attractive option. In addition, a wireless network user base will probably be much smaller, which allows an administrator to maintain a closer level of management on the policies and settings used to control the users.

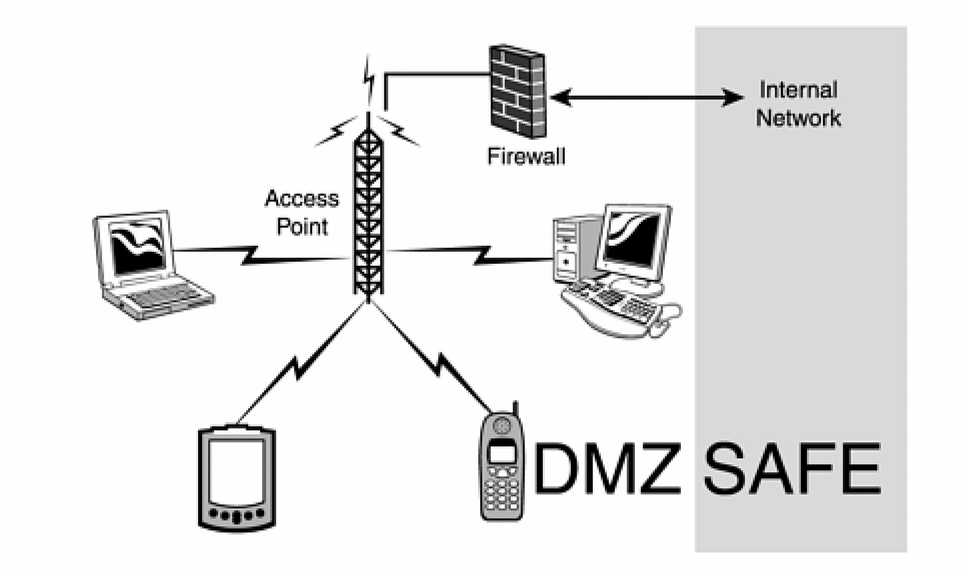


Fig – 6.8 Using a firewall with a DMZ.

6.2.2 VPNs

When discussing firewalls, it is also worth mentioning VPNs. A VPN, "Virtual Private Networks") is a virtual, encrypted network that is built on top of an existing network. This is also known as tunneling, because the encrypted data stream is set up and maintained within a normal, unencrypted connection. A VPN extends the safe internal network out to the remote user .Therefore, the remote wireless user exists in both networks at the same time. The wireless network remains available, but a VPN tunnel is created to connect the remote client to the internal network, thus making all the resources of the internal network available as well.

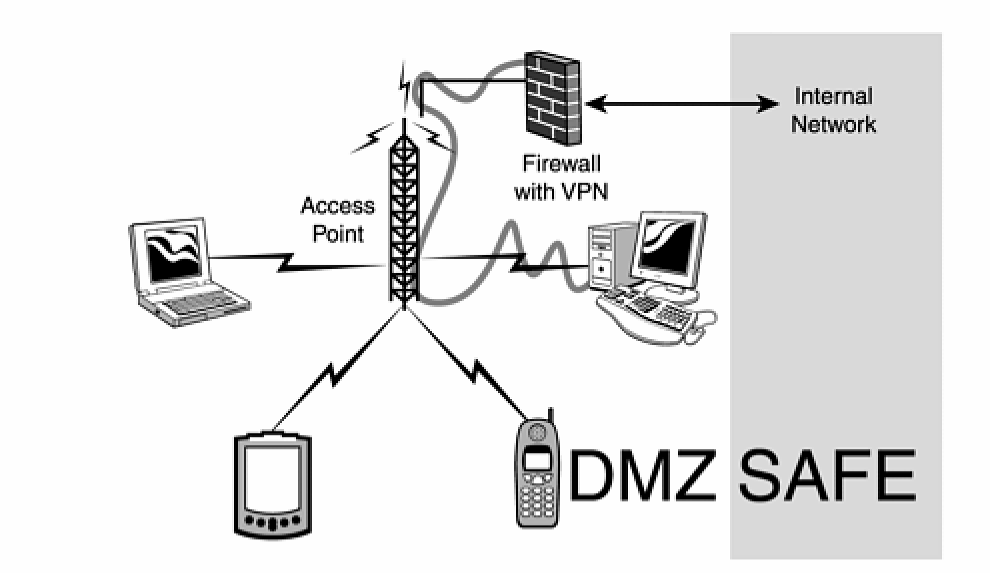


Fig - 6.9 DMZ with firewall and VPN tunnel between one client and the internal network.

The reason we need to discuss VPNs with firewalls is because they are often integrated into one appliance or software package. Because of this, a firewall can be set up to completely block all incoming requests, with the exception of authorized VPN clients. This will not only ensure a strong measure of security at the access point, but it will also provide an additional measure of security to the WLAN users and their data.

As you learned, the encryption used by most implementations of WEP is flawed. A cracker with a laptop and a Pringles can for an antenna can sit within the WLAN's radiation zone and capture enough data to crack the WEP password. By having this password, the cracker can then set up his computer to capture all data traveling through the air. Because he has the encryption password, he can decipher all the WEP-protected data and "see" the information. Email, documents, and passwords can all be gleaned this way.

However, by using VPN encryption in addition to the WEP encryption, a hacker would have to decipher the data twice. The first layer is the crackable WEP encryption, and the second layer is the robust VPN encryption. Because a hacker cannot easily reproduce the VPN's pass phrase, certificate, or smart card key, the success rate for cracking the VPN traffic will be very low.

Although using both a VPN and WEP is definitely to your advantage, there is a major downside. The problem arises as a result of the additional processing caused by encrypting and deciphering the data twice: first from WEP, and then from the VPN. Using WEP with VPN on a properly configured firewall/access point can affect transmission speed and throughput by as much as 80%. In other words, it would take 10 minutes to send a file over a VPN with WEP enabled, but it would only take 2 minutes without encryption. This impact can have serious consequences to network connectivity, and might all but eliminate the end user's enthusiasm for the wireless connection.

In addition, using VPN over wireless requires that client software be installed on every user's device. This requirement creates a few issues for end users. For example, most VPN software is written for the Windows platform. This means Macs, *nix-based computers, and palmtop computers might not be able to connect to the WLAN. Although this might not be an issue for most home and small businesses, it could have a serious impact on large or rapidly growing corporations.

6.2.3 RADIUS

Remote Authentication Dial-In User Service (RADIUS) is a protocol that is responsible for authenticating remote connections made to a system, providing authorization to network resources, and logging for accountability purposes. Although the protocol was actually developed years ago to help remote modem users securely connect to and authenticate with corporate networks, it has now evolved to the point where it can also be used in VPNs and WLANs to control almost every aspect of a user's connection.

There are several brands of RADIUS servers available. One of the more popular is Funk's Steel-Belted Radius server, which is often deployed with Lucent WLAN setups. Cisco has one, Microsoft has another, and there is even one called FreeRadius for *nix users. Regardless, they all work relatively the same.

6.3 WLAN Protection Enhancements

So far we have discussed generic solutions and tools. The following section will review specific tools to correct WEP-related vulnerabilities, as well as other security enhancements that are being considered for future versions of 802.11 networks.

6.3.1 TKIP

The Temporal Key Integrity Protocol (TKIP) is a more recent security feature offered by various vendors to correct the weak WEP problem. It was developed by some of the same researchers who found the weaknesses in how RC4 was implemented. TKIP corrects these weaknesses and more.

This new protocol still uses RC4 as the encryption algorithm, but it removes the weak key problem and forces a new key to be generated every 10,000 packets or 10kb, depending on the source. In addition, it hashes the initialization vector values that are sent as plaintext in the current release of WEP. This means the IVs are now encrypted, and are not as easy to sniff out of the air. Because the first three characters of the secret key are based on the three-character IV, the hashing of this value is a must. Without protecting the IV from casual sniffing attacks, a hacker can turn a 64-bit key (based on 8 characters x 8 bits in a byte) into a 40-bit key (based on 8 - 3 characters x 8 bits in a byte).

Also included in TKIP is a stronger and more secure method of verifying the integrity of the data. Called the Message Integrity Check, this part of TKIP closes a hole that would enable a hacker to inject data into a packet so he can more easily deduce the streaming key used to encrypt the data. Based on, "Cracking WEP," you know that if a hacker knows any two of the XOR values, he can calculate the third. Therefore, by injecting known data into a packet and capturing it after it has been encrypted, a hacker can determine the encrypted value and the plaintext value. When values are XORed together, the result is the PRGA streaming key. Once the PRGA for any packet is known, a hacker can reuse it to create his own encrypted packets without ever knowing the secret key. This is possible because the hacker can take the deduced PRGA value and XOR it with his choice of text. The result of this is a properly encrypted packet. He can then simply append the same IV value he pulled from the hacked packet and reapply it to the newly created packet. Thus, a hacker could completely bypass the creation of the KSA, which is the only part of the encryption process that requires the password.

This packet, once received by the access point, will be deciphered by using the appended IV values and the password used by the access point. Then the KSA is created, which is used to create the PRGA value that the hacker used to encrypt his packet. Then the PRGA streaming key is XORed with the encrypted packet, and that information is passed on.

With the new Message Integrity Check, this type of exploit is not possible. By verifying that the packet was not altered, and by dumping any packet that appears to be, the hacker will not be able to easily determine the PRGA. In addition, hashing the IVs creates yet another obstacle to any hacker that somehow deduces the PRGA. The hacker would have to determine the correct value of the hashed IVs, which is probably based on the data in the encrypted packet.

However, and even with all this extra security, TKIP is designed like the current version of WEP. This similarity allows TKIP to be backward-compatible with most hardware devices. This also means consumers merely have to update their firmware or software to bring their WLANs up to par.

Although this new security measure is important, it is only temporary. TKIP is more like a simple band-aid to patch the hemorrhaging artery of WEP security. This is because TKIP still operates under the condition that a hacker only has to crack one "password" to gain access to the WLAN. This is one of the major factors that caused the current release of WEP to be crackable. If WEP included a multifaceted security scheme using stronger encryption and/or multiple means of authentication, a hacker would have to attack the WLAN from several points, thus making WEP cracking much more difficult.

Therefore, if you own WLAN gear, keep a close eye on the vendor patch list to see when the update is released. You might also want to send an email to the vendors' support departments to get your name on an email notification list once they have a patch. If you do not own a WLAN and are looking to purchase one, consider looking for one with this option built into it. The only other option is to wait until the next standardized wireless products are released using the 802.11i standard.

6.3.2 AES

Advanced Encryption Standard (AES) is a newer encryption method that was selected by the U.S. government to replace DES as their standard. It is quite strong, and is actually under review for the next version of the wireless 802.11 standard (802.11i). In fact, although it is not yet officially supported in all WLAN hardware, certain vendors have already started implementing it.

AES uses an algorithm known as Rijndael. The algorithm was devised by Joan Daemen and Vincent Rijmen, and it became part of AES by a contest-like selection process that picked the best algorithm from proposed schemes created by the public sector. Other competitors were RSA (maker of RC4), IBM, and various international groups. The contest was hosted by the National Institute of Standards and Technology, which was working for the National Security Agency. The contest was devised as a result of the cracking of the previous standard encryption method (DES), which was broken in 1990. Because of this, an immediate replacement for the encryption method was a necessity. However, "immediate" in terms of a bureaucracy means that it took seven years to start the contest, and a few more years to actually select a winner. Thus, AES was born.

The strength of AES has yet to be truly tested. Barring advances in quantum computing, it is expected that AES will remain the standard form of encryption for many years. The following is a list of the number of guesses it would take to crack AES-protected data. There are three options, because AES allows different sizes of keys, depending on need. The key size directly reflects the strength of the encryption, as well as the amount of processing required to encrypt and decipher the text.

- 3.4×10^{38} possible 128-bit keys
- 6.2×10^{57} possible 192-bit keys
- 1.1×10^{77} possible 256-bit keys

In other words, using the same technology used to crack DES, it would take 149 trillion years to crack AES. Now, this was over a decade ago, but the fact remains that AES is a very good algorithm, and is expected to remain the standard for many decades to come. However, like all encryption, AES will be cracked eventually.

One downside to AES is that it has a larger overhead than RC4. This is because of the extra processing required during the encryption/decryption process, which is more complex than the relatively simple RC4. To illustrate, the entire RC4 algorithm is often coded in about 50 lines of code, whereas AES takes about 350 lines. Although this does make AES more of a resource hog, hardware accelerators and other software tricks can compensate for this.

Nevertheless, AES is destined to be the encryption method of all wireless traffic. Vendors are using AES already in their own proprietary WLANs, and this trend will act as a catalyst to make AES the official standard. However, you will not be able to use AES-ready hardware using the current standard of WEP. They are two entirely different encryption methods, and they will not work together.

6.3.3 SSL

Secure Sockets Layer is a protocol that has been in use for years online. The most popular form uses RC4 to encrypt data before it is sent over the Internet. This provides a layer of security to any sensitive data and has been incorporated into almost all facets of online communication. Everything from Web stores, online banking, Web-based email sites, and more use SSL to keep data secure. The reason why SSL is so important is because without encryption, anyone with access to the data pipeline can sniff and read the information as plaintext.

When building a secure WLAN, one of the important and necessary parts is authentication. Although there is some protection in the preshared password that is used to set up WEP, this will only encrypt the data. The flaw in this is that the system assumes the user is allowed to send data if the correct preshared password is used. In addition, by only using WEP (in conjunction with a DHCP WLAN), there is no way to track and monitor wireless users for security reasons. Thus, authentication of some sort is required.

Although authentication is important and necessary, it is also potentially vulnerable to several different types of attacks. For example, user authentication assumes that the person sending the password is indeed the owner of the account, which might not be true. Another weakness of an online authentication system is that the user information must be sent from the client to the host system. Therefore, the authentication information can be sniffed, which is why SSL is important to the authentication of users.

Because WLANs operate in a world that is meant to be very user-friendly and cross-platform, using proprietary software to encrypt and authenticate users would be tedious, and would be simply another obstacle for a user. Instead of designing an authentication system this way, many vendors are using a system that has been tried and tested for years. By using a Web browser with SSL enabled, an end user can make a secure and encrypted connection to a WLAN authentication server without having to deal with cumbersome software. As most wireless users will be familiar with using secure Web sites, the integration of SSL will go unnoticed. Once the connection is made, the user account information can be passed securely and safely.

6.3.4 IDSs

Intrusion detection systems (IDSs) are to computer networks what burglar alarms are to homes. The simple truth remains that all networks can be hacked. Because of this, we recommend that every network contain at least one form of IDS.

When dealing with wireless networks, using an IDS can be a bit tricky. Because of the nature of WLANs, guests might be connecting all the time and using the Internet or other network resources. Thus, an IDS system would quickly overload and eventually be ignored because of the number of false positives.

It is best to place the IDS on a system behind the firewall. This way, the amount of traffic it has to deal with is lessened, and it can become a reliable part of the security system. This is like trying to use a car alarm on a car that is parked next to the highway—the alarm would have a difficult time trying to distinguish a truck's rumbling from a thief's ministrations. Instead, you would want to park the car on the other side of the building or house to keep it from repeatedly having false alarms.

Thus, install an IDS and let it maintain a watchful eye over your network. Although this part of your security will not provide any direct protection, it does have significant advantages.

GLOSSARY

AP: Access Point. Any entity that has station functionality and provides access to the distribution services, via the wireless medium for associated stations.

Association Table: The Association table is within an AP and controls the routing of all packets between the Access Point and the wireless devices in a WLAN.

Basic Service Set: BSS is a collection, or set, of stations that are logically associated with each other and controlled by a single AP. Together, they operate as a fully connected wireless network.

Basic Service Set Identifier (BSSID): A 48-bit identifier used by all stations in a Basic Service Set as part of the frame header.

Beacon: A wireless LAN frame broadcast by access points that signals their availability.

Evil Twin Attack. An unauthorized AP whose goal is to masquerade as an existing legitimate/ authorized AP is called an Evil Twin. The evil twin AP is designed and located so that client stations receive stronger signals from it. Legitimate users are lured into the evil twin, and unknowingly give away user IDs and passwords.

Independent BSS: An IBSS is usually an ad-hoc network. In an IBSS, all of the stations are responsible for sending beacons.

IDS: Intrusion detection system.

MITM: Man in the middle. See Section 8.

Service Set Identifier (SSID): All APs and stations within the same wireless network use an identifier that is up to 32-bytes long.

Social Engineering: Social engineering is a term, coined in jest that refers to all non-technical methods of collecting information about a person so that the passwords the person may use can be predicted. The methods of collection range from dumpster diving, analyzing the publicly available information to making phone calls impersonating others.

STA: A wireless station.

WEP: Wired Equivalent Privacy (WEP) is a shared-secret key encryption system used to encrypt packets transmitted between a station and an AP.

References:

[1] Arbaugh, W.A., Shankar, N., Wang. J., and Zhang, K. Your 802.11 Network has No Clothes. Suntec City, Singapore.
http://citeseer.nj.nec.com/566520.html.

[2] Bellardo, J. and Savage, S. (August 2003). 802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions. Unpublished talk from University of California at San Diego.
http://www.cs.ucsd.edu/users/savage/papers/UsenixSec03.pdf

[3] Legon, Jeordan (March 2003). Get ready to tune in to wireless Net. CNN News.
http://www.cnn.com/2003/TECH/ptech/03/12/ wifi.growth/index.html

[4] Bing, Benny (2000). Performance Analysis. Broadband Wireless Access. Boston, MA: Kluwer Academic Pub.

[5] Asunción, Santamaría (2001). The Need for Standardization. Wireless LAN Standards and Applications. Boston, MA: Artech House.

[6] Asunción, Santamaría (2001). Future Trends. Wireless LAN Standards and Applications. Boston, MA: Artech House.

[7] Held, Gilbert (2001). Wireless LANs. Data Over Wireless Networks : Bluetooth, WAP, and Wireless LANS. NY: McGraw-Hill.

[8] Forouzan, Behrouz A (2003). Underlying Technologies. TCP/IP Protocol Suite. Boston, MA: McGraw-Hill.

[9] O'Hara, Bob (1999). The IEEE 802.11 Handbook: A Designer's Companion. NY: Standards Information Network, IEEE Press.

[10] Irvine, James (2002). Communication Systems. Data Communications and Networks: An Engineering Approach. NY: Wiley.

[11] Peterson, Larry L. (2000). The Physical Layer. Computer Networks: A Systems Approach. CA: Morgan Kaufmann Publishers.

[12] Asunción, Santamaría (2001). The Need for Standardization. Wireless LAN Standards and Applications. Boston, MA: Artech House.

[13] Irvine, James (2002). The Security Perspective. Data Communications and Networks : An engineering approach. NY: Wiley.

[14] Potter, Bruce (2003). 802.11 Security, CA: O'Reilly.

[15] Online Dictionary (March 2004). Person-in-Middle attack definition .

http://en.wikipedia.org/

[16] http://www.ciscopress.com/articles/article.asp?p=469624&seqNum=3&rl=1

[17] http://www.javvin.com/protocolWLAN.html

[18] John Bellardo and Stefan Savage, "802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions", 2003, Usenix 2003 Proceedings. http://www.cs.ucsd.edu/users/savage/papers/UsenixSec03.pdf Retrieved Jan 20, 2004.

[19] Jon Edney and William A. Arbaugh, Real 802.11 Security: Wi-Fi Protected Access and 802.11i, 480 pages, Addison Wesley, 2003, ISBN: 0-321-13620-9

[20] Jamil Farshchi, Wireless Intrusion Detection Systems, November 5, 2003, http://www.securityfocus.com/infocus/1742 Retrieved Jan 20, 2004

[21] Bob Fleck and Jordan Dimov, "Wireless Access Points and ARP Poisoning: Wireless vulnerabilities that expose the wired network," October 2001. http://www.cigitallabs.com/resources/papers/download/arppoison.pdf. Retrieved on Jan 20, 2004.

[22] Rob Flickenger, Wireless Hacks: 100 Industrial-Strength Tips & Tools, 286 pages, O'Reilly & Associates, September 2003, ISBN: 0-596-00559-8

[23] Matthew S. Gast, 802.11 Wireless Networks: The Definitive Guide, 464 pages, O'Reilly & Associates, April 2002, ISBN: 0596001835.

[24] Vikram Gupta, Srikanth Krishnamurthy, and Michalis Faloutsos, "Denial of Service Attacks at the MAC Layer in Wireless Ad Hoc Networks", Proceedings of 2002 MILCOM Conference, Anaheim, CA, October 2002.

[25] Chris Hurley, Michael Puchol, Russ Rogers, and Frank Thornton, WarDriving: Drive, Detect, Defend, A Guide to Wireless Security, ISBN: 1931836035, Syngress, 2004.

[26] IEEE, IEEE 802.11 standards documents, http://standards.ieee.org/wireless/ . Retrieved Jan 20, 2004

[27] Tom Karygiannis and Les Owens, Wireless Network Security: 802.11, Bluetooth and Handheld Devices, National Institute of Standards and Technology Special Publication 800-48, November 2002. http://cs-www.ncsl.nist.gov/publications/ nistpubs/800-48/NIST_SP_800-48.pdf . Retrieved Jan 20, 2004

[28] Prabhaker Mateti, TCP/IP Suite, The Internet Encyclopedia, Hossein Bidgoli (Editor), John Wiley 2003, ISBN 0471222011.

[29] Robert Moskowitz, “Debunking the Myth of SSID Hiding”, Retrieved on March 10, 2004. http://www.icsalabs.com/html/communities/WLAN/wp_ssid_hiding. pdf.

[30] Bruce Potter and Bob Fleck, 802.11 Security, O'Reilly & Associates, 2002; ISBN: 0-596-00290-4.

[31] William Stallings, Wireless Communications & Networks, Prentice Hall, 2001, ISBN: 0130408646.

[32] War-chalking, http://www.warchalking.org/. Retrieved Jan 20, 2004.

[33] Joshua Wright, “Detecting Wireless LAN MAC Address Spoofing”, Retrieved on Jan 20, 2004. http://home.jwu.edu/jwright/