Chapter 8

Cisco Wireless Security

Solutions in this chapter:

- Understanding Security Fundamentals and Principles of Protection
- MAC Filtering
- Reviewing the Role of Policy
- Implementing WEP
- Addressing Common Risks and Threats
- Sniffing, Interception, and Eavesdropping
- Spoofing and Unauthorized Access
- Network Hijacking and Modification
- Denial of Service and Flooding Attacks

☑ Summary

☑ Solutions Fast Track

☑ Frequently Asked Questions

Introduction

There is not much indication of anything slowing down the creation and deployment of new technology to the world any time in the near future. With the constant pressure to deploy the latest generation of technology today, little time is allowed for a full and proper security review of the technology and components that make it up.

This rush to deploy, along with the insufficient security review, not only allows age-old security vulnerabilities to be reintroduced to products, but creates new and unknown security challenges as well. Wireless networking is not exempt from this, and like many other technologies, security flaws have been identified and new methods of exploiting these flaws are published regularly.

Utilizing security fundamentals developed over the last few decades, you can review and protect your wireless networks from known and unknown threats. In this chapter, we recall security fundamentals and principles that are the foundation of any good security strategy, addressing a range of issues from authentication and authorization, to controls and audit.

No primer on security would be complete without an examination of the common security standards, which are addressed in this chapter alongside the emerging privacy standards and their implications for the wireless exchange of information.

We also look at how you can maximize the features of existing security standards like Wired Equivalent Protocol (WEP). We also examine the effectiveness of Media Access Control (MAC) and protocol filtering as a way of minimizing opportunity. Lastly, we look at the security advantages of using virtual private networks (VPNs) on a wireless network, as well as discuss the importance of convincing users of the role they can play as key users of the network.

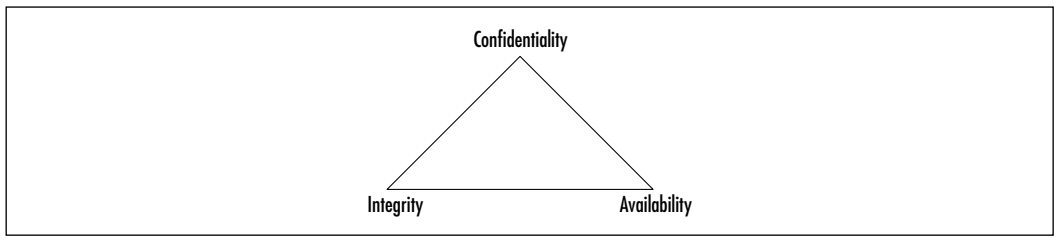
You'll also learn about the existing and anticipated threats to wireless networks, and the principles of protection that are fundamental to a wireless security strategy. And although many of the attacks are similar in nature to attacks on wired networks, you need to understand the particular tools and techniques that attackers use to take advantage of the unique way wireless networks are designed, deployed, and maintained. We explore the attacks that have exposed the vulnerabilities of wireless networks, and in particular the weaknesses inherent in the security standards. Through a detailed examination of these standards, we identify how these weaknesses have lead to the development of new tools and tricks that hackers use to exploit your wireless networks. We look at the emergence and

threat of "war driving" technique and how it is usually the first step in an attack on wireless networks.

Understanding Security Fundamentals and Principles of Protection

Security protection starts with the preservation of the *confidentiality*, *integrity*, and *availability* (CIA) of data and computing resources. These three tenets of information security, often referred to as "The Big Three," are sometimes represented by the CIA triad, shown in Figure 8.1.

Figure 8.1 The CIA Triad



As we describe each of these tenets, you will see that in order to provide for a reliable and secure wireless environment, you will need to ensure that each tenet is properly protected. To ensure the preservation of The Big Three and protect the privacy of those whose data is stored and flows through these data and computing resources, The Big Three security tenets are implemented through tried-and-true security practices. These other practices enforce The Big Three by ensuring proper authentication for authorized access while allowing for nonrepudiation in identification and resource usage methods, and by permitting complete accountability for all activity through audit trails and logs. Some security practitioners refer to Authentication, Authorization, and Audit (accountability) as "AAA." Each of these practices provides the security implementer with tools which they can use to properly identify and mitigate any possible risks to The Big Three.

Ensuring Confidentiality

Confidentiality attempts to prevent the intentional or unintentional unauthorized disclosure of communications between a sender and recipient. In the physical world, ensuring confidentiality can be accomplished by simply securing the physical area. However, as evidenced by bank robberies and military invasions, threats

exist to the security of the physical realm that can compromise security and confidentiality.

The moment electronic means of communication were introduced, many new possible avenues of disclosing the information within these communications were created. The confidentiality of early analog communication systems, such as the telegraph and telephone, were easily compromised by simply having someone connect to the wires used by a sender and receiver.

When digital communications became available, like with many technologies, it was only a matter of time until knowledgeable people were able to build devices and methods that could interpret the digital signals and convert them to whatever form needed to disclose what was communicated. And as technology grew and became less expensive, the equipment needed to monitor and disclose digital communications became available to anyone wishing to put the effort into monitoring communication.

With the advent of wireless communications, the need for physically connecting to a communication channel to listen in or capture confidential communications was removed. Although you can achieve some security by using extremely tight beam directional antennas, someone still just has to sit somewhere in between the antennas to be able to monitor and possibly connect to the communications channel without having to actually tie into any physical device.

Having knowledge that communications channels are possibly compromised allows us to properly implement our policies and procedures to mitigate the wireless risk. The solution used to ensure The Big Three and other security tenets is *encryption*.

The current implementation of encryption in today's wireless networks use the RC4 stream cipher to encrypt the transmitted network packets, and the WEP to protect authentication into wireless networks by network devices connecting to them (that is, the network adapter authentication, not the user utilizing the network resources). Both of which, due mainly to improper implementations, have introduced sufficient problems that have made it possible to determine keys used and then either falsely authenticate to the network or decrypt the traffic traveling across through the wireless network.

With these apparent problems, those in charge of wireless network security should utilize other proven and properly implemented encryption solutions, such as Secure Shell (SSH), Secure Sockets Layer (SSL), or IPSec.

Ensuring Integrity

Integrity ensures the accuracy and completeness of information throughout its process methods. The first communication methods available to computers did not have much in place to ensure the integrity of the data transferred from one to another. As such, occasionally something as simple as static on a telephone line could cause the transfer of data to be corrupted.

To solve this problem, the idea of a checksum was introduced. A *checksum* is nothing more than taking the message you are sending and running it through a function that returns a simple value which is then appended to the message being sent. When the receiver gets the complete message, they would then run the message through the same function and compare the value they generate with the value that was included at the end of the message.

The functions that are generally used to generate basic checksums are usually based upon simple addition or modulus functions. These functions can sometimes have their own issues, such as the function not being detailed enough to allow for distinctly separate data that could possibly have identical checksums. It is even possible to have two errors within the data itself cause the checksum to provide a valid check because the two errors effectively cancel each other out. These problems are usually addressed through a more complex algorithm used to create the digital checksum.

Cyclic redundancy checks (CRCs) were developed as one of the more advanced methods of ensuring data integrity. CRC algorithms basically treat a message as an enormous binary number, whereupon another large fixed binary number then divides this binary number. The remainder from this division is the checksum. Using the remainder of a long division as the checksum, as opposed to the original data summation, adds a significant chaos to the checksum created, increasing the likelihood that the checksum will not be repeatable with any other separate data stream.

These more advanced checksum methods, however, have their own set of problems. As Ross Williams wrote in his 1993 paper, A Painless Guide to CRC Error Detection Algorithms (www.ross.net/crc/crcpaper.html), the goal of error detection is to protect against corruption introduced by noise in a data transfer. This is good if we are concerned only with protecting against possible transmission errors. However, the algorithm provides no means of ensuring the integrity of an intentionally corrupted data stream. If someone has knowledge of a particular data stream, altering the contents of the data and completing the transaction with a valid checksum is possible. The receiver would not have knowledge of the

changes in the data because their checksum would match and it would appear as if the data was transferred with no errors.

This form of intentional integrity violation is called a "Data Injection." In such cases, the best way to protect data is to (once again) use a more advanced form of integrity protection utilizing cryptography. Today, this higher level of protection is generally provided through a stronger cryptographic algorithm such as the MD5 or RC4 ciphers.

Wireless networks today use the RC4 stream cipher to protect the data transmitted as well as provide for data integrity. It has been proven that the 802.11 implementation of the RC4 cipher with its key scheduling algorithm introduces enough information to provide a hacker with enough to be able to predict your network's secret encryption key. Once the hacker has your key, they are not only able to gain access to your wireless network, but also view it as if there was no encryption at all.

Ensuring Availability

Availability, as defined in an information security context, ensures that access data or computing resources needed by appropriate personnel is both reliable and available in a timely manner. The origins of the Internet itself come from the need to ensure the availability of network resources. In 1957, the United States Department of Defense (DoD) created the Advanced Research Projects Agency (ARPA) following the Soviet launch of Sputnik. Fearing loss of command and control over U.S. nuclear missiles and bombers due to communication channel disruption caused by nuclear or conventional attacks, the U.S. Air Force commissioned a study on how to create a network that could function with the loss of access or routing points. Out of this, packet switched networking was created, and the first four nodes of ARPANET were deployed in 1968 running at the then incredibly high speed of 50 kilobits per second.

The initial design of packet switched networks did not take into consideration the possibility of an actual attack on the network from one of its own nodes. As the ARPANET grew into what we now know as the Internet, many modifications have been made to the protocols and applications that make up the network, ensuring the availability of all resources provided.

Wireless networks are experiencing many similar design issues, and due to the proliferation of new wireless high-tech devices, many are finding themselves in conflict with other wireless resources. Like their wired equivalents, there was little expectation that conflicts would occur within the wireless spectrum available for

use. Because of this, very few wireless equipment providers planned their implementations with features to ensure the availability of the wireless resource in case a conflict occurred.

Ensuring Privacy

Privacy is the assurance that the information a customer provides to some party will remain private and protected. This information generally contains customer personal nonpublic information that is protected by both regulation and civil liability law. Your wireless policy and procedures should contain definitions on how to ensure the privacy of customer information that might be accessed or transmitted by your wireless networks. The principles and methods here provide ways of ensuring the protection of the data that travels across your networks and computers.

Ensuring Authentication

Authentication provides for a sender and receiver of information to validate each other as the appropriate entity they are wishing to work with. If entities wishing to communicate cannot properly authenticate each other, then there can be no trust of the activities or information provided by either party. It is only through a trusted and secure method of authentication that we are able to provide for a trusted and secure communication or activity.

The simplest form of authentication is the transmission of a shared password between the entities wishing to authenticate with each other. This could be as simple as a secret handshake or a key. As with all simple forms of protection, once knowledge of the secret key or handshake was disclosed to nontrusted parties, there could be no trust in who was using the secrets anymore.

Many methods can be used to acquire a simple secret key, from something as simple as tricking someone into disclosing it, to high-tech monitoring of communications between parties to intercept the key as it is passed from one party to the other. However the code is acquired, once it is in a nontrusted party's hands, they are able to utilize it to falsely authenticate and identify themselves as a valid party, forging false communications, or utilizing the user's access to gain permissions to the available resources.

The original digital authentication systems simply shared a secret key across the network with the entity they wished to authenticate with. Applications such as Telnet, File Transfer Protocol (FTP), and POP-mail are examples of programs that simply transmit the password, in clear-text, to the party they are authenticating

with. The problem with this method of authentication is that anyone who is able to monitor the network could possibly capture the secret key and then use it to authenticate themselves as you in order to access these same services. They could then access your information directly, or corrupt any information you send to other parties. They may even be able to attempt to gain higher privileged access with your stolen authentication information.

Configuring & Implementing…

Clear-Text Authentication

Clear-text (non-encrypted) authentication is still widely used by many people today who receive their e-mail through the Post Office Protocol (POP), which by default sends the password unprotected in clear-text from the mail client to the server. You can protect your e-mail account password in several ways, including connection encryption as well as not transmitting the password in clear-text through the network by hashing with MD5 or some similar algorithm.

Encrypting the connection between the mail client and server is the only way of truly protecting your mail authentication password. This will prevent anyone from capturing your password or any of the mail you might transfer to your client. SSL is generally the method used to encrypt the connection stream from the mail client to the server and is supported by most mail clients today.

If you just protect the password through MD5 or a similar cryptocipher, anyone who happens to intercept your "protected" password could identify it through a brute force attack. A brute force attack is where someone generates every possible combination of characters running each version through the same algorithm used to encrypt the original password until a match is made and your password is found.

Authentication POP (APOP) is a method used to provide password-only encryption for mail authentication. It employs a challenge/response method defined in RFC1725 that uses a shared timestamp provided by the server being authenticated to. The timestamp is hashed with the username and the shared secret key through the MD5 algorithm.

There are still a few problems with this, the first of which is that all values are known in advance except the shared secret key. Because of this, there is nothing to provide protection against a brute-force attack

Continued

on the shared key. Another problem is that this security method attempts to protect your password. Nothing is done to prevent anyone who might be listening to your network from then viewing your e-mail as it is downloaded to your mail client.

You can find an example of a brute-force password dictionary generator that can produce a brute-force dictionary from specific character sets at www.dmzs.com/tools/files.

To solve the problem of authentication through sharing common secret keys across an untrusted network, the concept of Zero Knowledge Passwords was created. The idea of Zero Knowledge Passwords is that the parties who wish to authenticate each other want to prove to one another that they know the shared secret, and yet not share the secret with each other in case the other party truly doesn't have knowledge of the password, while at the same time preventing anyone who may intercept the communications between the parties from gaining knowledge as to the secret that is being used.

Public-key cryptography has been shown to be the strongest method of doing Zero Knowledge Passwords. It was originally developed by Whitfield Diffie and Martin Hellman and presented to the world at the 1976 National Computer Conference. Their concept was published a few months later in their paper, New Directions in Cryptography. Another crypto-researcher named Ralph Merkle, working independently from Diffie and Hellman, also invented a similar method for providing public-key cryptography, but his research was not published until 1978.

Public-key cryptography introduced the concept of having keys work in pairs, an encryption key and a decryption key, and having them created in such a way that generating one key from the other is infeasible. The encryption key is then made public to anyone wishing to encrypt a message to the holder of the secret decryption key. Because identifying or creating the decryption key from the encryption key is infeasible, anyone who happens to have the encrypted message and the encryption key will be unable to decrypt the message or determine the decryption key needed to decrypt the message.

Public-key encryption generally stores the keys or uses a certificate hierarchy. The certificates are rarely changed and often used just for encrypting data, not authentication. Zero Knowledge Password protocols, on the other hand, tend to use Ephemeral keys. *Ephemeral keys* are temporary keys that are randomly created for a single authentication, and then discarded once the authentication is completed.

Note that the public-key encryption is still susceptible to a chosen-ciphertext attack. This attack is where someone already knows what the decrypted message is and has knowledge of the key used to generate the encrypted message. Knowing the decrypted form of the message lets the attacker possibly deduce what the secret decryption key could be. This attack is unlikely to occur with authentication systems because the attacker will not have knowledge of the decrypted message: your password. If they had that, they would already have the ability to authenticate as you and not need to determine your secret decryption key.

Currently 802.11 network authentication is centered on the authentication of the wireless device, not on authenticating the user or station utilizing the wireless network. Public-key encryption is not used in the wireless encryption process. Although a few wireless vendors have dynamic keys that are changed with every connection, most wireless 802.11 vendors utilize shared-key authentication with static keys.

Shared key authentication is utilized by WEP functions with the following steps:

1. When a station requests service, it sends an authentication frame to the access point (AP) it wishes to communicate with.
2. The receiving AP replies to the authentication frame with its own, which contains 128 octets of challenge text.
3. The station requesting access encrypts the challenge text with the shared encryption key and returns to the AP.
4. The access decrypts the encrypted challenge using the shared key and compares it with the original challenge text. If they match, an authentication acknowledgement is sent to the station requesting access, otherwise a negative authentication notice is sent.

As you can see, this authentication method does not authenticate the user or any resource the user might need to access. It is only a verification that the wireless device has knowledge of the shared secret key that the wireless AP has. Once a user has passed the AP authentication challenge, that user will then have full access to whatever devices and networks the AP is connected to. You should still use secure authentication methods to access any of these devices and prevent unauthorized access and use by people who might be able to attach to your wireless network.

To solve this lack of external authentication, the IEEE 802.11 committee is working on 802.1x, a standard that will provide a framework for 802-based

networks authenticating from centralized servers. Back in November 2000, Cisco introduced Light Extensible Authentication Protocol (LEAP) authentication to their wireless products, which adds several enhancements to the 802.11 authentication system, including the following:

- Mutual authentication utilizing Remote Access Dial-In User Service (RADIUS).
- Securing the secret key with one-way hashes that make password reply attacks impossible.
- Policies to force the user to re-authenticate more often, getting a new session key with each new session. This will help to prevent attacks where traffic is injected into the data stream.
- Changes to the initialization vector used in WEP encryption that make the current exploits of WEP ineffective.

Not all vendors support these solutions, so your best bet is to protect your network and servers with your own strong authentication and authorization rules.

Extensible Authentication Protocol (EAP)

The Extensible Authentication Protocol (EAP) was designed to provide authentication methods within the Point-to-Point-Protocol (PPP). EAP allows for the integration of third-party authentication packages that use PPP. EAP can be configured so that it can support a number of methods for authentication schemes, such as token cards, public key, certificates, PINs, and on and on.

When you install PPP/EAP, EAP will not select a specific authentication method at the Link Control Protocol (LCP) Phase, but will wait until the Authentication Phase to begin. What this does is allow the authenticator the ability to request more information, and with this information it will decide on the method of authentication to use. This delay will also allow for the implementation of a server on the backend that can control the various authentication methods while the PPP authenticator passes through the authentication exchange.

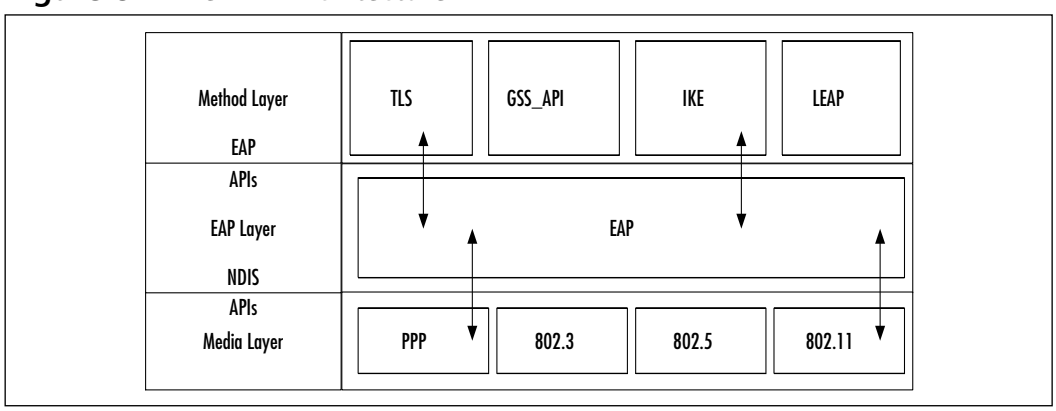
In this way, network devices like APs or switches do not need to understand each request type, because they will simply act as a conduit, or passthrough agent, for a server on a host. The network device will only need to see if the packet has the success or failure code in order to terminate the authentication phase.

EAP is able to define one or more requests for peer-to-peer authentication. This can happen because the request packet includes a type field, such as Generic Token, one-time password (OTP), or an MD5 challenge. The MD5 challenge is very similar to the Challenge Handshake Authentication Protocol (CHAP).

EAP is able to provide you with a flexible, link-layer security framework (see Figure 8.2), by having the following features:

- EAP mechanisms are IETF standards–based and allow for the growth of new authentication types when your security needs change:
  - Transport Layer Security (TLS)
  - Internet Key Exchange (IKE)
  - GSS_API (Kerberos)
  - Other authentication schemes (LEAP)
- There is no dependency on IP, because this is an encapsulation protocol.
- There is no windowing as this is a simple ACK/NAK protocol.
- No support for fragmentation.
- Can run over any link layer (PPP, 802.3, 802.5, 802.11, and so on).
- Does not consider a physically secure link as an authentication method to provide security.
- Assumes that there is no reordering of packets.
- Retransmission of packets is the responsibility of authenticator.

Figure 8.2 The EAP Architecture



802.1x and EAP

One type of wireless security is focused on providing centralized authentication and dynamic key distribution area. By using the IEEE 802.1x standard, the EAP, and the Cisco Lightweight Extensible Authentication Protocol (LEAP) as an end-to-end solution, you can provide enhanced functionality to your wireless network. Two main elements are involved in using this standard:

- EAP/LEAP allows all wireless client adapters the capability to communicate with different authentication servers such as RADIUS and Terminal Access Controller Access Control System (TACACS+) servers that are located on the network.
- You implement the IEEE 802.1x standard for network access control that is port based for MAC filtering.

When these features are deployed together, wireless clients that are associated with APs will not be able to gain access to the network unless the user performs a network logon. The user will need to enter a username and password for network logon, after which the client and a RADIUS server will perform authentication, hopefully leading to the client being authenticated by the supplied username and password and access to the network and resources.

How this occurs is that the RADIUS server and client device will then receive a client-specific WEP key that is used by the client for that specific logon session. As an added level of security, the user's password and session key will never be transmitted in the open, over the wireless connection.

Here is how Authentication works and the WEP key is passed:

1. The wireless client will associate with an AP located on the wireless network.
2. The AP will then prevent all other attempts made by that client to gain access to network until the client logs on to the network.
3. The client will supply a username and password for network logon.
4. Using 802.1x standard and EAP/LEAP, the wireless client and a RADIUS server perform authentication through the AP. The client will then use a one-way hash of the user-supplied password as a response to the challenge, and this will be sent to the RADIUS server. The RADIUS server will then reference its user table and compare that to the response from the client. If there is a match, the RADIUS server

authenticates the client, and the process will be repeated, but in reverse. This will enable the client to authenticate the RADIUS server.

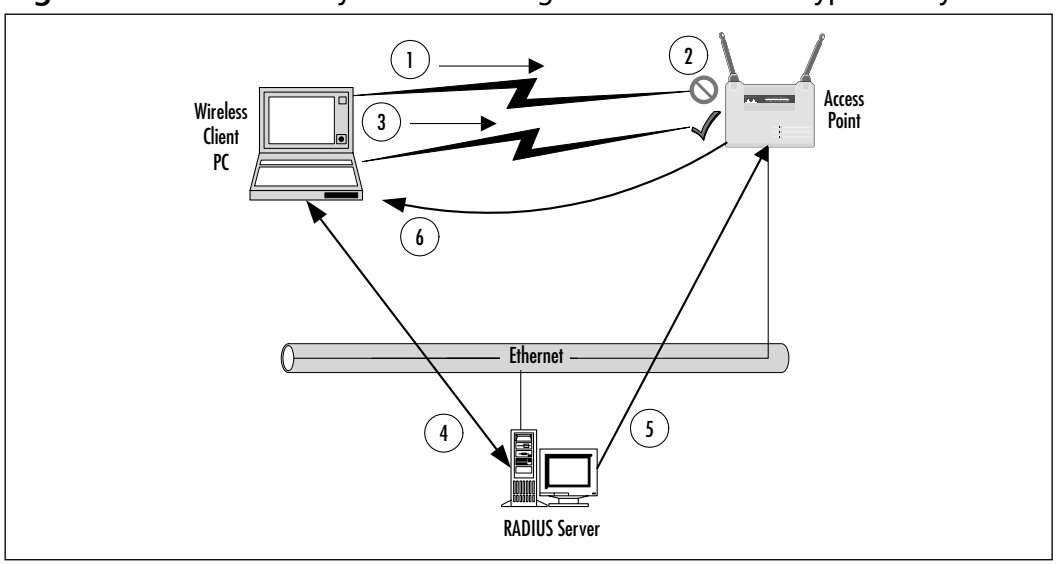
(If you are using LEAP, the RADIUS server will send an authentication challenge to the client.)

After authentication completes successfully, the following steps take place:

1. The RADIUS server and the client determine a WEP key that is unique for the client and that session.
2. The RADIUS server transmits this WEP key (also known as a session key), across the wired LAN to the AP.
3. The AP will encrypt the broadcast key and the session key so that it can then send the new encrypted key to the client. The client will then use the session key to decrypt it.
4. The client and AP then activates the WEP. The APs and clients will then use the session and broadcast WEP keys for all communications that occur during the session.
5. For enhanced security, the session key and broadcast key are regularly changed at regular periods that are configured in the RADIUS server.

A more simplified version is included in Figure 8.3.

Figure 8.3 Cisco Security Solution Using Session-Based Encryption Keys



An Introduction to the 802.1x Standard

In order to better understand 802.1x, you must also understand the enhancements of current IEEE 802.11b security products and features. The current IEEE 802.11b standard is severely limited because it is available only for the current open and shared key authentication scheme, which is non-extensible.

Some of these requirements for the future security include the following:

- The creation of new 802.11 authentication methods.
- These authentication methods must be independent of the underlying 802.11 hardware.
- Authentication methods should be dynamic because hard coding it makes it difficult to fix security holes when they are found.
- It must have the ability to support Public Key Infrastructure (PKI) and certificate schemes.

Project Authorization Request (PAR) for 802.1x

Currently, no standard mechanism allows access to and from a network segment based only on the authenticated state of a port user. The problem is that network connectivity allows for the anonymous access to company data and the Internet. When 802-based networks are deployed in more accessible areas, you will need a method to authenticate and authorize basic network access. These types of projects provide for common interoperable solutions that use standards-based authentication and authorization infrastructures like those that are commonly supporting schemes such as dial-up access already.

The Objectives of the 802.1x Standard

The IEEE 802.1x Working Group was created for the purpose of providing a security framework for port-based access control that resides in the upper layers. The most common method for port-based access control is to enable new authentication and key management methods without changing current network devices.

The benefits that are the end result of this group are as follows:

- There is a significant decrease in hardware cost and complexity.
- There are more options, which allows you to pick and choose your security solution.

- You can install the latest and greatest security technology, and it should still work with your existing infrastructure.
- You are able to respond to security issues as quickly as they arise.

802.1x in a Nutshell

When a client device connects to a port on an 802.1x switch and AP, the switch port can determine the authenticity of the devices. Due to this and, according to the protocol specified by 802.1x, the services offered by the switch can be made available on that port. Only EAPOL (see the following list) frames can be sent and received on that port until the authentication is complete. When the device is properly authentication, the port switches traffic as though it were a regular port.

Here is some terminology for the 802.1x standard that you should familiarize yourself with:

- **Port** A port is a single point of connection to the network.
- **Port Access Entity (PAE)** The PAE controls the algorithms and protocols that are associated with the authentication mechanisms for a port.
- **Authenticator PAE** The authenticator PAE enforces authentication before it will allow access resources located off of that port.
- **Supplicant PAE** The supplicant PAE tries to accesses the services that are allowed by the authenticator.
- **Authentication Server** The Authentication Server is used to verify the supplicant PAE. It decides whether the supplicant is authorized to access the authenticator or not.
- **Extensible Authentication Protocol Over LAN (EAPOL)** The 802.1x defines a standard for encapsulating EAP messages so that they can be handled directly by a LAN MAC service. 802.1x tries to make authentication more encompassing, rather than enforcing specific mechanisms on the devices. Because of this, 802.1x uses Extensible Authentication Protocol to receive authentication information.
- **Extensible Authentication Protocol Over Wireless (EAPOW)** When EAPOL messages are encapsulated over 802.11 wireless frames, they are known as EAPOW.

Making it Come Together—User Identification and Strong Authentication

With the addition of the 802.1x standard, clients are identified by usernames, not the MAC address of the devices. This was designed to not only enhance security, but to streamline the process for authentication, authorization, and accountability for your network. 802.1x was designed so that it could support extended forms of authentication, using password methods (such as one-time passwords, or GSS_API mechanisms like Kerberos) and nonpassword methods (such as biometrics, Internet Key Exchange [IKE], and smart cards).

Key Derivation Can Be Dynamic

You can also use per-user session keys, because the 802.1x standard allows for the creation of them. Because you don't need to keep WEP keys at the client device or AP, you can dispense per-user, and/or per session–based WEP keys. These WEP keys will be dynamically created at the client for every session, thus making it more secure. The Global key, like a broadcast WEP key, can be encrypted using a unicast session key and then sent from the AP to the client in a much more secure manner.

Mutual Authentication

When using 802.1x and EAP, you should use some form of mutual authentication. This will make the client and the authentication servers mutually authenticating end-points and will assist in the mitigation of attacks from man in the middle types of devices. To enable mutual authentication, you could use any of the following EAP methods:

- **TLS** This requires that the server supply a certificate and establish that it has possession of the private key.
- **IKE** This requires that the server show possession of preshared key or private key (this can be considered certificate authentication).
- **GSS_API (Kerberos)** This requires that the server can demonstrate knowledge of the session key.

NOTE

Cisco Systems has also created a lightweight mutual authentication scheme, called LEAP (discussed later), so that your network is able to support operating systems that do not normally support EAP. LEAP also offers the capability to have alternate certificate schemes such as EAP-TLS.

Per-Packet Authentication

EAP can support per-packet authentication and integrity protection, but this authentication and integrity protection is not extended to all types of EAP messages. For example, NAK (negative acknowledgment) and notification messages are not able to use per-packet authentication and integrity. Per-packet authentication and integrity protection works for the following (packet is encrypted unless otherwise noted):

- TLS and IKE derive session key
- TLS ciphersuite negotiations (not encrypted)
- IKE ciphersuite negotiations
- Kerberos tickets
- Success and failure messages that use derived session key (through WEP)

Designing & Planning…

Preventing Dictionary Attacks Using EAP

EAP was designed to support extended authentication. When you implement EAP, you can avoid dictionary attacks by using nonpassword-based schemes such as biometrics, certificates, OTP, smart cards, and token cards.

You should be sure that if you are using password-based schemes that they use some form of mutual authentication so that they are more protected against dictionary attacks.

Possible Implementation of EAP on the WLAN

There are two main authentication methods for EAP on your wireless LAN: One is EAP-MD5, and the other is to use Public Key Infrastructure (PKI) with EAP-TLS. EAP-MD5 has a couple of issues because it does not support the capability for mutual authentication between the access server and the wireless client. The PKI schemes also has drawbacks, because it is very computation-intensive on the client systems, you need a high degree of planning and design to make sure that your network is capable of supporting PKI, and it is not cheap.

Cisco Light Extensible Authentication Protocol (LEAP)

LEAP is an enhancement to the EAP protocol, and as you remember, the EAP protocol was created in an effort to provide a scalable method for a PPP-based server to authenticate its clients and, hopefully allow for mutual authentication. An extensible packet exchange should allow for the passing of authentication information between the client devices and the PPP servers. The thing is that PPP servers usually rely on a centralized authentication server system that can validate the clients for them. This is where a RADIUS or a TACACS+ server usually comes into play.

This reason that the servers can work is that the servers have a protocol that will enable them to pass EAP packets between the authentication server and the PPP server. Essentially this makes the PPP server a passthrough or a relay agent, so that the authentication process happens between the client and the RADIUS server. The RADIUS server will then tell the PPP server the results of the authentication process (pass/fail) that will allow the client to access the network and its resources.

To make sure that all types of network access servers could be implemented to validate clients to network resources, the EAP protocol was created. Because we are talking about wireless connections though, the link between the AP and the client is not PPP but WLAN.

When the 802.11 specifications were standardized, it allowed for the encryption of data traffic between APs and clients through the use of a WEP encryption key. When it was first implemented, the AP would have a single key, and this key had to be configured on each client. All traffic would be encrypted using this single key. Well, this type of security has a lot of issues. In current implementations that use EAP authentication, the client and RADIUS server have a shared

secret; generally this is some permutation of a username and password combination. The server will then pass certain information to the AP so that the client and AP can derive encryption keys that are unique for this client-AP pair. This is called Cisco LEAP authentication.

The previous section discussed the implementation methods of EAP (EAP-MD5, and PKI with EAP-TLS), and some of the issues that you can expect to see when you plan to implement them. LEAP may be a better option because it can offer mutual authentication, it needs only minimal support from the client's CPU, it can support embedded systems, and it can support clients whose operating system does not have the support for native EAP or allow for the use of the PKI authentication.

LEAP authentication works through three phases: the *start phase*, the *authenticate phase*, and the *finish phase*. The following sections show the process that the client and AP go through so that the client can also talk to the RADIUS server.

Start Phase for LEAP Authentication

In the start phase, information (in packet form) is transferred between the client and APs:

1. The EAPOW-Start (this is also called EAPOL-Start in 802.1x for wired networks) starts the authentication process. This packed is sent from the client to the AP.
2. The EAP-Request/Identity is sent from the AP to the client with a request for the clients Identity.
3. The EAP-Response/Identity is sent from the client to the AP with the required information.

Authentication Phase for LEAP Authentication

This sequence will change based on the mutual authentication method you choose for the client and the authentication server. If you were to use TLS for the transfer of certificates in a PKI deployment, EAP-TLS messages will be used, but because we are talking about LEAP, it would go more like this:

1. The client sends an EAP-Response/Identity message to the RADIUS server through the AP as a RADIUS-Access-Request with EAP extensions.
2. The RADIUS server then returns access-request with a RADIUS-challenge, to which the client must respond.

Cisco LEAP authentication is a mutual authentication method, and the AP is only a passthrough. The AP in the authenticate phase forwards the contents of the packets from EAP to RADIUS and from Radius to EAP.

The (Big) Finish Phase of LEAP Authentication

The steps for the finish phase are as follows:

1. If the client is considered invalid, the RADIUS server will send a RADIUS deny packet with an EAP fail packet embedded within it. If the client is considered to be valid, the server will send a RADIUS request packet with an EAP success attribute.
2. The RADIUS-Access-Accept packet contains the MS-MPPE-Send-Key attribute to the AP, where it obtains the session key that will be used by client.

The RADIUS server and client both create a session key from the user's password, when using LEAP. The encryption for the IEEE 802.11 standard can be based on a 40/64-bit or 104/128-bit key. Note that the key derivation process will create a key that is longer than is required. This is so that when the AP receives the key from the RADIUS server (using MS-MPPE-Send-Key attribute), it will send an EAPOL-KEY message to the client. This key will tell the client the key length and what key index that it should use.

The key value isn't sent because the client has already created it on its own WEP key. The data packet is then encrypted using the full-length key. The AP will also send an EAPOL-KEY message that gives information about the length, key index, and value of the multicast key. This message is encrypted using the full-length session unicast key from the AP.

Configuration and Deployment of LEAP

In this section, we talk about the installation and requirements for a LEAP solution that consists of a client, an AP and a RADIUS server for key distribution in your network.

Client Support for LEAP

You can configure your client to use LEAP mode in one of two modes:

- **Network Logon Mode** In Network Logon Mode, an integrated network logon provides for a single-sign on for both the wireless network

as well as Microsoft Networking. This will provide users with a transparent security experience. This is probably the most common method of authenticating into the wireless network (or the wired network).

- **Device Mode** In Device Mode, the wireless LAN stores the username/password identification, so that you can get non-interactive authentication into the wireless LAN. You will often see this on wireless appliances where the devices that can authenticate themselves through these preconfigured credentials are enough security.

Access Point Support for LEAP

Access points can provide 802.1x for 802.11 Authenticator support. In order to make this work, you need to take the following two steps in setting up 802.1x authenticator support:

- You need to configure the AP to use 40/64- or 104/128-bit WEP mode.
- You must give the LEAP RADIUS server address and configure the shared secret key that the AP and RADIUS server use, so that they can communicate securely.

Configuring your RADIUS server for LEAP

To configure the RADIUS server for authentication and key distribution users, you will need to do the following:

- You need to create the user databases.
- You need to configure the APs as Network Access Servers (NASs). This will enable users that are configured with Cisco-Aironet RADIUS extensions on the NAS to use RADIUS. RADIUS requests from the AP with EAP extensions are passed as described earlier.

Ensuring Authorization

Authorization is the rights and permissions granted to a user or application that enables access to a network or computing resource. Once a user has been properly identified and authenticated, authorization levels determine the extent of system rights that the user has access to.

Many of the early operating systems and applications deployed had very small authorization groups. Generally, only user groups and operator groups were

available for defining a user's access level. Once more formal methods for approaching various authorization levels were defined, applications and servers started offering more discrete authorization levels. You can observe this by simply looking at any standard back-office application deployed today.

Many of them provide varying levels of access for users and administrators. For example, they could have several levels of user accounts allowing some users access to just view the information, while giving others the ability to update or query that information and have administrative accounts based on the authorization levels needed (such as being able to look up only specific types of customers, or run particular reports while other accounts have the ability to edit and create new accounts).

As shown in the previous authentication example, Cisco and others have implemented RADIUS authentication for their wireless devices. Now, utilizing stronger authentication methods, you can implement your authorization policies into your wireless deployments.

However, many wireless devices do not currently support external authorization validation. Plus, most deployments just ensure authorized access to the device. They do not control access to or from specific network segments. To fully restrict authorized users to the network devices they are authorized to utilize, you will still need to deploy an adaptive firewall between the AP and your network.

This is what was done earlier this year by two researchers at NASA (for more information, see www.nas.nasa.gov/Groups/Networks/Projects/Wireless). To protect their infrastructure, but still provide access through wireless, they deployed a firewall segmenting their wireless and department network. They most likely hardened their wireless interfaces to the extent of the equipments' possibilities by utilizing the strongest encryption available to them, disabling SID broadcast, and allowing only authorized MAC addresses on the wireless network.

They then utilized the Dynamic Host Configuration Protocol (DHCP) on the firewall, and disabled it on their AP. This allowed them to expressly define which MAC addresses could receive an IP address, and what the lease lifetime of the IP address would be.

The researchers then went on to turn off all routing and forwarding between the wireless interface and the internal network. If anyone happened to be able to connect to the wireless network, they would still have no access to the rest of the computing resources of the department. Anyone wishing to gain further access would have to go to an SSL protected Web site on the firewall server and authenticate as a valid user. The Web server would authenticate the user against a local

RADIUS server, but they could have easily used any other form of user authentication (NT, SecurID, and so on).

Once the user was properly authenticated, the firewall would change the firewall rules for the IP address that user was supposed to be assigned to, allowing full access to only the network resources they are authorized to access.

Finally, once the lease expired or was released for any reason from the DHCP assigned IP address, the firewall rules would be removed and that user and their IP would have to re-authenticate through the Web interface to allow access to the network resources again.

MAC Filtering

In order to fully discuss the advantages and disadvantages of MAC filtering, let's have a short review on what a MAC address is. The term *MAC* stands for Media Access Control, and forms the lower layer in the Data-Link layer of the OSI model. The purpose of the MAC sublayer is to present a uniform interface between the physical networking media (copper/fiber/radio frequency) and the Logical Link Control portion of the Data-Link layer. These two layers are found onboard a NIC, whether integrated into a device or used as an add-on (PCI card or PCMCIA card).

What Is a MAC Address?

In order to facilitate delivery of network traffic, the MAC layer is assigned a unique address, which is programmed into the NIC at the time of manufacture. The operating system will associate an IP address with this MAC address, which allows the device to participate in an IP network. Because no other NIC in the world should have the same MAC address, it is easy to see why it could be a secure way to equate a specific user with the MAC address on his or her machine.

Now, let's look at an actual MAC address. For example, my laptop has a MAC address of 00-00-86-4C-75-48. The first three octets are called the organizationally unique identifier (OUI). The Institute of Electrical and Electronic Engineers controls these OUIs and assigns them to companies as needed. If you look up the 00-00-86 OUI on the IEEE's Web site (http://standards.ieee.org/regauth/oui/index.shtml), it will state that the manufacturer of this NIC is the 3Com Corporation.

Corporations can own several OUIs, and often acquire additional OUIs when they purchase other companies. For example, when Cisco purchased Aironet

Wireless Communications in 1999, they added the 00-40-96 OUI to the many others they have.

Some other OUIs you could see on your WLAN might be the following:

- **00-02-2D** Agere Communications (previously known as ORiNOCO)
- **00-10-E7** Breezecom
- **00-E0-03** Nokia Wireless
- **00-04-5A** Linksys

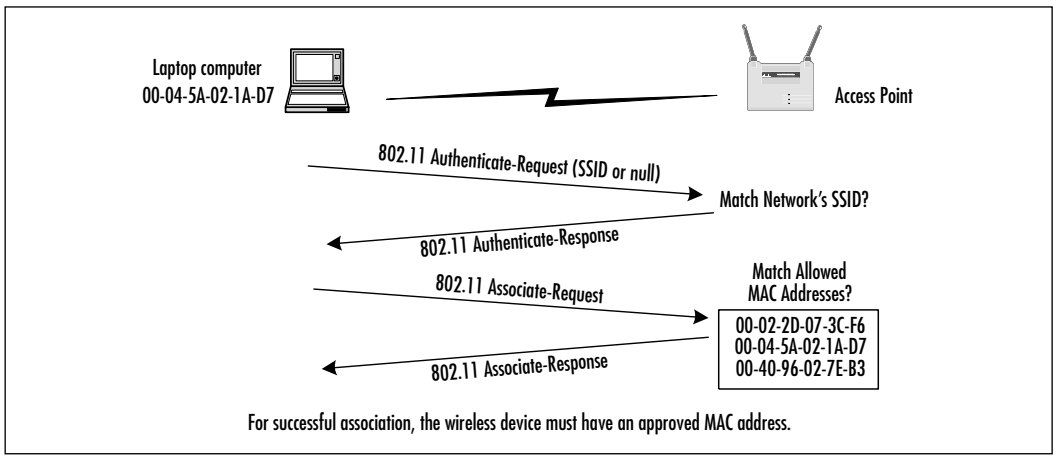
The remaining three octets in a MAC address are usually burned into the NIC during manufacture, thus assuring that duplicate addresses will not exist on a network. We say "usually" because this rule has a few exceptions. For example, in some redundancy situations, one NIC on a machine is able to assume the MAC address of the other NIC if the primary NIC fails. Some early 802.11 PCMCIA cards also had the capability to change their MAC address. Although not necessarily easy to do, changing the MAC address gives a user the ability to spoof the MAC address of another PCMCIA card. This could be used to circumvent MAC filtering or be employed in a denial of service (DoS) attack against a specific user.

Where in the Authentication/Association Process Does MAC Filtering Occur?

When a wireless device wants to connect to a WLAN, it goes though a two-part process called authentication and authorization. After both have been completed, the device is allowed access to the WLAN.

As mentioned earlier, when a wireless device is attempting to connect to a WLAN, it sends an authentication request to the AP (see Figure 8.4). This request will contain the SSID of the target network, or a null value if connecting to an open system. The AP will grant or deny authentication based on this string. Following a successful authentication, the requesting device will attempt to associate with the AP. It is at this point in time that MAC filtering plays its role. Depending on the AP vendor and administrative setup of the AP, MAC filtering either allows only the specified MAC addresses—blocking the rest, or it allows all MAC addresses—blocking specifically noted MACs. If the MAC address is allowed, the requesting device is allowed to associate with the AP.

Figure 8.4 MAC Filtering



Determining MAC Filtering Is Enabled

The easiest way to determine if a device has failed the association process due to MAC filtering is through the use of a protocol analyzer, like Sniffer Pro or AiroPeek. The difficulty here is that other factors besides MAC filtering could prevent association from occurring. RADIUS or 802.1x authentication, or an incorrect WEP key could also prevent this. These of course are costly mechanisms commonly seen in large corporate environments. Due to the costs involved with setting up the higher forms of non-AP-based authentication, most small businesses or home installations will use MAC filtering to limit access (if they use anything at all).

MAC Spoofing

If you discover that your MAC address is not allowed to associate with the AP, don't give up. There are other ways into the network besides the front door.

First off, just because you can't associate with the AP doesn't mean you can't sit there and passively watch the traffic. With 802.11b protocol analysis software, your laptop can see all the other stations' communication with any AP within range. Because the MAC addresses of the other stations are transmitted in clear text, it should be easy to start compiling a list of the MAC addresses allowed on the network.

Some early runs of 802.11 PCMCIA cards had the capability to modify their MAC addresses. Depending on the card and the level of firmware, the method to

change your MAC address may vary. There are sites on the Internet that can give you more specific information on altering these parameters.

Once you have modified the MAC address, you should be able to associate it with the AP. Keep in mind however, that if the device bearing the MAC address you have stolen is still operating on the network, you will not be able to use your device. To allow the operation of two duplicate MAC addresses will break ARP tables and will attract a level of attention to your activities that is undesirable. The advanced hacker we are discussing would realize this. In attempts to subvert the security mechanisms, traffic would be monitored to sufficiently pattern the intended victim whose MAC address and identification are to be forged in order to avoid detection.

Ensuring Non-Repudiation

Repudiation is defined by West's Encyclopedia of American Law as "the rejection or refusal of a duty, relation, right or privilege." A repudiation of a transaction or contract means that one of the parties refuses to honor their obligation to the other as specified by the contract. Non-repudiation could then be defined as the ability to deny, with irrefutable evidence, a false rejection or refusal of an obligation.

In their paper "Non-Repudiation in the Digital Environment," Adrian McCullagh and William Caelli put forth an excellent review of the traditional model of non-repudiation and the current trends for crypto-technical non-repudiation. The paper was published online by First Monday—you can find it at www.firstmonday.dk/issues/issue5_8/mccullagh/index.html.

The basis for a repudiation of a traditional contract is sometimes associated with the belief that the signature binding a contract is a forgery, or that the signature is not a forgery but was obtained via unconscionable conduct by a party to the transaction, by fraud instigated by a third party, or undue influence exerted by a third party. In typical cases of fraud or repudiated contracts, the general rule of evidence is that if a person denies a particular signature, the burden of proving that the signature is valid falls upon the receiving party.

Common law trust mechanisms establish that in order to overcome false claims of non-repudiation, a trusted third party needs to act as a witness to the signature being affixed. Having a witness to the signature of a document, who is independent of the transactions taking place, reduces the likelihood that a signor is able to successfully allege that the signature is a forgery. However, there is always the possibility that the signatory will be able to deny the signature on the basis of the situations listed in the preceding paragraph.

A perfect example of a non-repudiation of submissions can be viewed by examining the process around sending and receiving registered mail. When you send a registered letter, you are given a receipt containing an identification number for the piece of mail sent. If the recipient claims that the mail was not sent, the receipt is proof that provides the non-repudiation of the submission. If a receipt is available with the recipient's signature, this provides the proof for the non-repudiation of the delivery service. The postal service provides the non-repudiation of transport service by acting as a Trusted Third Party (TTP).

Non-repudiation, in technical terms, has come to mean the following:

- In authentication, a service that provides proof of the integrity and origin of data both in an unforgeable relationship, which can be verified by any third party at any time; or
- In authentication, an authentication that with high assurance can be asserted to be genuine, and that cannot subsequently be refuted.

The Australian Federal Government's Electronic Commerce Expert group further adopted this technical meaning in their 1998 report to the Australian Federal Attorney General as:

> Non-repudiation is a property achieved through cryptographic methods which prevents an individual or entity from denying having performed a particular action related to data (such as mechanisms for non-rejection or authority (origin); for proof of obligation, intent, or commitment; or for proof of ownership.

In the digital realm, a movement is in place to shift the responsibility of proving that a digital signature is invalid to the owner of the signature, not the receiver of the signature, as is typically used in traditional common law methods.

In only a few examples does the burden of proof fall upon the alleged signer. One such example is usually found in taxation cases where the taxpayer has made specific claims and as such is in a better position to disprove the revenue collecting body's case. Another example would be in an instance of negligence. In a negligence action, if a plaintiff is able to prove that a defendant failed to meet their commitment, the burden of proof is in effect shifted to the defendant to establish that they have met their obligations.

The problem found in the new digital repudiation definitions that have been created is that they take into consideration only the validity of the signature itself. They do not allow for the possibility that the signor was tricked or forced into

signing, or that their private key may be compromised, allowing the forgery of digital signatures.

With all the recent cases of Internet worms and viruses, it is not hard to imagine that one might be specifically built to steal private keys. A virus could be something as simple as a Visual Basic macro attached to a Word document, or an e-mail message that would search the targets hard drive looking for commonly named and located private key rings that could then be e-mailed or uploaded to some rogue location.

With this and other possible attacks to the private keys, it becomes difficult, under the common law position, for someone attempting to prove the identity of an alleged signatory. This common law position was established and founded in a paper-based environment where witnessing became the trusted mechanism utilized to prevent the non-repudiation of a signature. For a digital signature to be proven valid, however, it will need to be established through a fully trusted mechanism.

Thus, for a digitally signed contract to be trusted and not susceptible to repudiation, the entire document handling and signature process must take place within a secured and trusted computing environment. As we will see in some of the documentation to follow, the security policies and definitions created over the years have established a set of requirements necessary to create a secure and trusted computer system.

If we follow the definitions established in the Information Technology Security Evaluation Certification (ITSEC) to create a trusted computing environment of at least E3 to enforce functions and design of the signing process and thus prevent unauthorized access to the private key, the common law position for digitally signed documents can be maintained. E3 also ensures that the signing function is the only function able to be performed by the signing mechanism by having the source code evaluated to ensure that this is the only process available through the code. If these security features are implemented, it can be adequately assessed that under this mechanism the private key has not been stolen and as such that any digital signature created under this model has the trust established to ensure the TTP witness and validation of any signature created, preventing any possible repudiation from the signor.

One such example of a secure infrastructure designed and deployed to attempt to provide a digitally secure TTP are the PKI systems available for users of unsecure public networks such as the Internet. PKI consists of a secure computing system that acts as a certificate authority (CA) to issue and verify digital certificates. Digital certificates contain the public key and other identification information needed to verify the validity of the certificate. As long as the trust in

the CA is maintained (and with it, the trust in the security of the private key), the digital certificates issued by the CA and the documents signed by them remain trusted. As long as the trust is ensured, then the CA acts as a TTP and provides for the non-repudiation of signatures created by entities with digital certificates issued through the CA.

Accounting and Audit Trails

Auditing provides methods for tracking and logging activities on networks and systems, and it links these activities to specific user accounts or sources of activity. In case of simple mistakes or software failures, audit trails can be extremely useful in restoring data integrity. They are also a requirement for trusted systems to ensure that the activity of authorized individuals on the trusted system can be traced to their specific actions, and that those actions comply with defined policy. They also allow for a method of collecting evidence to support any investigation into improper or illegal activities.

Most modern database applications support some level of transaction log detailing the activities that occurred within the database. This log could then be used to either rebuild the database if it had any errors or create a duplicate database at another location. To provide this detailed level of transactional logging, database logging tends to consume a great deal of drive space for its enormous log file. This intense logging is not needed for most applications, so you will generally have only basic informative messages utilized in system resource logging.

The logging features provided on most networks and systems involve the logging of known or partially known resource event activities. Although these logs are sometimes used for analyzing system problems, they are also useful for those whose duty it is to process the log files and check for both valid and invalid system activities.

To assist in catching mistakes and reducing the likelihood of fraudulent activities, the activities of a process should be split among several people. This segmentation of duties allows the next person in line to possibly correct problems simply because they are being viewed with fresh eyes.

From a security point of view, segmentation of duties requires the collusion of at least two people to perform any unauthorized activities. The following guidelines assist in assuring that the duties are split so as to offer no way other than collusion to perform invalid activities:

- **No access to sensitive combinations of capabilities** A classic example of this is control of inventory data and physical inventory. By

separating the physical inventory control from the inventory data control, you remove the unnecessary temptation for an employee to steal from inventory and then alter the data so that the theft is left hidden.

- **Prohibit conversion and concealment** Another violation that can be prevented by segregation is ensuring that supervision is provided for people who have access to assets. An example of an activity that could be prevented if properly segmented follows a lone operator of a night shift. This operator, without supervision, could copy (or "convert") customer lists and then sell them off to interested parties. Instances have been reported of operators actually using the employer's computer to run a service bureau at night.
- **The same person cannot both originate and approve transactions** When someone is able to enter and authorize their own expenses, it introduces the possibility that they might fraudulently enter invalid expenses for their own gain.

These principles, whether manual or electronic, form the basis for why audit logs are retained. They also identify why people other than those performing the activities reported in the log should be the ones who analyze the data in the log file.

In keeping with the idea of segmentation, as you deploy your audit trails, be sure to have your logs sent to a secure, trusted, location that is separate and non-accessible from the devices you are monitoring. This will help ensure that if any inappropriate activity occurs, the person can't falsify the log to state that the actions did not take place.

Most wireless APs do not offer any method of logging activity, but if your equipment provides the feature, you should enable it and then monitor it for inappropriate activity using tools such as logcheck. Wireless AP logging should, if it's available, log any new wireless device with its MAC address upon valid WEP authentication. It should also log any attempts to access or modify the AP itself.

Using Encryption

Encryption has always played a key role in information security, and has been the center of controversy in the design of the WEP wireless standard. But despite the drawbacks, encryption will continue to play a major role in wireless security, especially with the adoption of new and better encryption algorithms and key management systems.

As we have seen in reviewing the basic concepts of security, many of the principles used to ensure the confidentiality, integrity, and availability of servers and services are through the use of some form of trusted and tested encryption. We also have seen that even with encryption, if we get tied up too much in the acceptance of the hard mathematics as evidence of validity, it is possible to be tricked into accepting invalid authorization or authentication attempts by someone who has been able to corrupt the encryption system itself by either acquiring the private key through cryptanalysis or stealing the private key from the end user directly.

Cryptography offers the obvious advantage that the material it protects cannot be used without the keys needed to unlock it. As long as those keys are protected, the material remains protected. There are a few potential disadvantages to encryption as well. For instance, if the key is lost, the data becomes unavailable, and if the key is stolen, the data becomes accessible to the thief.

The process of encryption also introduces possible performance degradation. When a message is to be sent encrypted, time must be spent to first encrypt the information, then store and transmit the encrypted data, and then later decode it. In theory, this can slow a system by as much as a factor of three.

Until recently, distribution and use of strong encryption was limited and controlled by most governments. The United States government had encryption listed as munitions, right next to cruise missiles! As such, it was very difficult to legally acquire and use strong encryption through the entire Internet. With the new changes in trade laws, however, it is now possible to use stronger encryption for internal use as well as with communications with customers and other third parties.

Encrypting Voice Data

Voice communications have traditionally been a very simple medium to intercept and monitor. When digital cell and wireless phones arrived, there was a momentary window in which monitoring voice communications across these digital connections was difficult. Today, the only equipment needed to monitor cell phones or digital wireless telephones can be acquired at a local Radio Shack for generally less than $100.

Most voice communication systems are not designed to ensure the privacy of the conversations on them, so a new industry was created to facilitate those needs. Originally designed for government and military usage, telephone encryption devices give people the option of encrypting their daily calls. A few of these devices are starting to make their way into the commercial market. Although a

few are being slowed down by organizations such as the National Security Agency (NSA) and the Federal Bureau of Investigation (FBI), who argue that it will prevent their "legal" monitoring of criminal activities, consumer market needs should eventually push these devices into the mainstream.

The Internet, being a communications network, offers people the ability to communicate with anyone, anywhere. Because of this, it didn't take long for the appearance of applications enabling voice communications across the Internet. Many of the early versions, like all budding technologies, did not offer any protection methods for their users. As a result, people utilizing Internet voice communications programs could have their communications monitored by someone with access to the data stream between parties. Fortunately, encryption is making its way into some of these programs, and if you're careful, you should be able to find one that uses modern tested and secure encryption algorithms such as Twofish, a popular and publicly-available encryption algorithm created by Bruce Schneier.

Encrypting Data Systems

Data networks have traditionally been susceptible to threats from a trusted insider. However, as soon as someone connects their network to another entity, it introduces possible security compromises from outside sources. Remember, all forms of data communications, from simple modem lines to frame-relay and fiber-optic connections, can be monitored.

Reviewing the Role of Policy

Good policy is your first line of defense. A properly designed policy examines every threat (or tries to) and ensures that confidentiality, integrity, and availability are maintained (or at least cites the known and accepted risks). As we shall see, policy definition begins with a clear identification and labeling of resources being utilized that will build into specific standards that define acceptable use in what's considered an authorized and secure manner. Once a basic standard is defined, you start building specific guidelines and procedures for individual applications and services.

Many wireless manufacturers have responded to security threats hampering their initial product versions by releasing upgrades to their software and drivers. Your security policy should always require that all technology, either existing or newly deployed, have the latest security patches and upgrades installed in a timely manner. However, because the development and release of patches takes time,

policy and its proper implementation tend to be the first layer of defense when confronting known and unknown threats.

A well-written policy should be more than just a list of recommended procedures. It should be an essential and fundamental element of your organization's security practices. A good policy can provide protection from liability due to an employee's actions, or can form a basis for the control of trade secrets. A policy or standard should also continue to grow and expand as new threats and technologies become available. They should be constructed with the input of an entire organization and audited both internally and externally to ensure that the assets they are protecting have the controls in place as specified in the standards, policies, and guidelines.

Designing & Planning…

The Management Commitment

Management must be aware of their needed commitment to the security of corporate assets, which includes protection of information. Measures must be taken to protect it from unauthorized modification, destruction, or disclosure (whether accidental or intentional), and ensure its authenticity, integrity, availability and confidentiality.

Fundamental to the success of any security program is senior management's commitment to the information security process and their understanding of how important security controls and protections are to the enterprise's continuity.

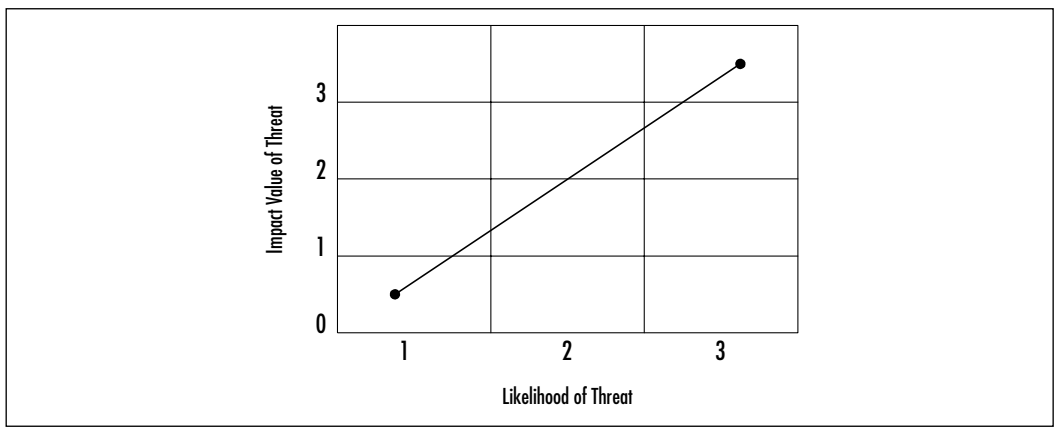
The senior management statement usually contains the following elements:

- An acknowledgment of the importance of computing resources to the business model
- A statement of support for information security throughout the enterprise
- A commitment to authorize and manage the definition of the lower level standards, procedures, and guidelines

Part of any policy definition includes what is required to ensure that the policy is adhered to. The prime object of policy controls is to reduce the effect of security threats and vulnerabilities to the resources being protected. The policy definition process generally entails the identification of what impact a threat would have on an organization, and what the likelihood of that threat occurring would be. Risk analysis (RA) is the process of analyzing a threat and producing a representative value of that threat.

Figure 8.5 displays a matrix created using a small x–y graph representing the threat and the corresponding likelihood of that threat. The goal of RA is to reduce the level of impact and the likelihood that it will occur. A properly implemented control should move the plotted point from the upper right to the lower left of the graph.

Figure 8.5 Threat versus Likelihood Matrix



An improperly designed and implemented control will show little to no movement in the plotted point before and after the control's implementation.

Identifying Resources

To assess and protect resources, they must first be identified, classified, and labeled so that in the process of performing your risk analysis you are able to document all possible risks to each identified item and provide possible solutions to mitigate those risks.

Security classification provides the following benefits:

- Demonstrates an organization's commitment to security procedures

- Helps identify which information is the most sensitive or vital to an organization
- Supports the tenets of confidentiality, integrity, and availability as it pertains to data
- Helps identify which protections apply to which information
- May be required for regulatory, compliance, or legal reasons

In the public sector, the common categories utilized in the classification of resources are the following:

- **Public** These are no-risk items that can be disclosed to anyone, as long as they do not violate any individual's right to privacy, and knowledge of this information does not expose an organization to financial loss or embarrassment, or jeopardize security assets. Examples of public information include marketing brochures, published annual reports, business cards, and press releases.
- **Internal Use** These are low-risk items that due to their technical or business sensitivity are limited to an organization's employees and those contractors covered by a nondisclosure agreement. Should there be unauthorized disclosure, compromise, or destruction of the documents, there would only be minimal impact on the organization, its customers, or employees. Examples of Internal Use information include employee handbooks, telephone directories, organizational charts, and policies.
- **Confidential** These are moderate-risk items whose unauthorized disclosure, compromise, or destruction would directly or indirectly impact an organization, its customers, or employees, possibly causing financial damage to an organization's reputation, a loss of business, and potential legal action. They are intended solely for use within an organization and are limited to those individuals who have a "need-to-know" security clearance. Examples of confidential items include system requirements or configurations, proprietary software, personnel records, customer records, business plans, budget information, and security plans and standards.
- **Restricted** These are high-risk critical items whose unauthorized disclosure, compromise, or destruction would result in severe damage to a company, providing significant advantages to a competitor, or causing penalties to the organization, its customers, or employees. It is intended solely for restricted use within the organization and is limited to those

with an explicit, predetermined, and stringent "business-need-to-know." Examples of restricted data include strategic plans, encryption keys, authentication information (passwords, PINs, and so on), and IP addresses for security-related servers.

All information, whether in paper, spoken, or electronic form should be classified, labeled, and distributed in accordance to your information classification and handling procedures. This will assist in the determination of what items have the largest threat, and as such, should determine how you set about providing controls for those threats.

Your wireless network contains a few internal items that should be identified and classified, however the overall classification of any network device comes down the level of information that flows through its channels. While using e-mail systems or accessing external sites through your wireless network, you will likely find that your entire network contains restricted information. However, if you are able to encrypt the password, the classification of your network data will then be rated based upon the non-authentication information traveling across your wireless network.

Understanding Classification Criteria

To assist in your risk analysis, you can use a few additional criteria to determine the classification of information resources:

- **Value** Value is the most commonly used criteria for classifying data in the private sector. If something is valuable to an individual or organization, that will prompt the data to be properly identified and classified.
- **Age** Information is occasionally reclassified to a lower level as time passes. In many government organizations, some classified documents are automatically declassified after a predetermined time period has passed.
- **Useful Life** If information has become obsolete due to new information or resources, it is usually reclassified.
- **Personal Association** If information is associated with specific individuals or is covered under privacy law, it may need to be reclassified at some point.

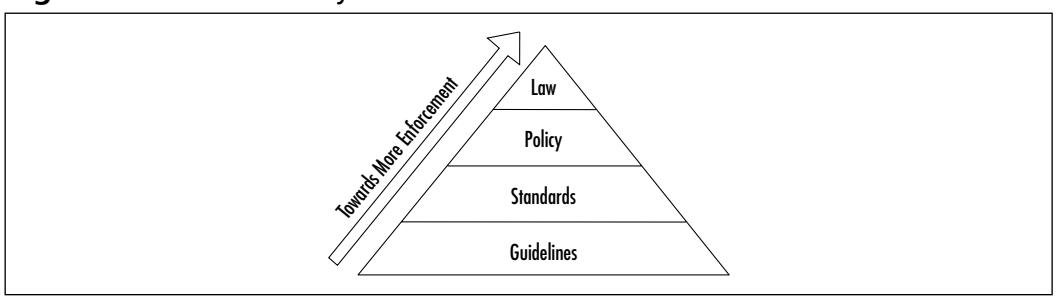
Implementing Policy

Information classification procedures offer several steps in establishing a classification system, which provides the first step in the creation of your security standards and policies. The following are the primary procedural steps used in establishing a classification system:

1. Identify the administrator or custodian.
2. Specify the criteria of how the information will be classified and labeled.
3. Classify the data by its owner, who is subject to review by a supervisor.
4. Specify and document any exceptions to the classification policy.
5. Specify the controls that will be applied to each classification level.
6. Specify the termination procedures for declassifying the information or for transferring custody of the information to another entity.
7. Create an enterprise awareness program about the classification controls.

Once your information and resources are properly identified and classified, you will be able to define the controls necessary to ensure the privacy and security of information regarding your employees and customers. Many industries are required, either by regulation or civil law, to ensure that proper policy is in place to protect the security and privacy of nonpublic personal information. This relationship of policy, guidelines, and legal standards is shown in Figure 8.6.

Figure 8.6 The Hierarchy of Rules



Guidelines refer to the methodologies of securing systems. Guidelines are more flexible than standards or policies and take the varying nature of information systems into consideration as they are developed and deployed, usually offering specific processes for the secure use of information resources. Many organizations have general security guidelines regarding a variety of platforms

available within them: NT, SCO-Unix, Debian Linux, Red Hat Linux, Oracle, and so on.

Standards specify the use of specific technologies in a uniform way. Although they are often not as flexible as guidelines, they do offer wider views to the technology specified. Usually, standards are in place for general computer use, encryption use, information classification, and others.

Policies are generally statements created for strategic or legal reasons, from which the standards and guidelines are defined. Some policies are based on legal requirements placed on industries such as health insurance, or they can be based upon common law requirements for organizations retaining personal nonpublic information of their customers.

Policies, standards, and guidelines must be explicit and focused, and they must effectively communicate the following subjects:

- Responsibility and authority
- Access control
- The extent to which formal verification is required
- Discretionary/mandatory control (generally relevant only in government or formal policy situations)
- Marking/labeling
- Control of media
- Import and export of data
- Security and classification levels
- Treatment of system output

The intent of policy is to delineate what an organization expects in the information security realm. Reasonable policy should also reflect any relevant laws and regulations that impact the use of information within an organization.

The System Administration, Networking, and Security Institute (SANS) offers excellent resources for implementing security standards, policies, and guidelines. You can find more information on policy implementation at the SANS Web site at www.sans.org/newlook/resources/policies/policies.htm. There you'll find example policies regarding encryption use, acceptable use, analog/ISDN lines, anti-virus software, application service providers, audits, and many others.

In this section's sidebar, "Sample Wireless Communication Policy," you will find the example wireless policy that defines the standards used for wireless communications.

Designing & Planning…

Sample Wireless Communication Policy

1.0 Purpose

This policy prohibits access to <*Company Name*> networks via unsecured wireless communication mechanisms. Only wireless systems that meet the criteria of this policy or have been granted an exclusive waiver by InfoSec are approved for connectivity to <*Company Name*>'s networks.

2.0 Scope

This policy covers all wireless data communication devices (for example, personal computers, cellular phones, PDAs, and so on) connected to any of <*Company Name*>'s internal networks. This includes any form of wireless communication device capable of transmitting packet data. Wireless devices and/or networks without any connectivity to <*Company Name*>'s networks do not fall under the purview of this policy.

3.0 Policy

To comply with this policy, wireless implementations must: maintain point-to-point hardware encryption of at least 56 bits; maintain a hardware address that can be registered and tracked (for instance, a MAC address); support strong user authentication which checks against an external database such as TACACS+, RADIUS, or something similar.

Exception: a limited-duration waiver to this policy for Aironet products has been approved if specific implementation instructions are followed for corporate and home installations.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Terms	Definitions
User Authentication	A method by which the user of a wireless system can be verified as a legitimate user independent of the computer or operating system being used.

6.0 Revision History

Addressing the Issues with Policy

Wireless users have unique needs that policy must address. The administrator must take diligent care in creating effective policy to protect the users, their data, and corporate assets. But just what is an effective policy for wireless users? Let's look at some common sense examples of good wireless policy.

First, wireless LANs are an "edge" technology. As such, policy should reflect a standard consistent with end users attempting to gain access to network resources from "the edge." In the case of wired LANs, typically you would set some standard physical access restrictions. This type of restriction would protect the LAN from certain types of attacks. You might also create group policy on the PC for authentication and access restrictions to corporate domains, and so long as there is no inside threat, the LAN is secured. (This scenario is unlikely in that disgruntled employees are representative of a solid portion of network hacking/misuse.) If you can't physically access the media, you cannot break in. If you do not furnish a valid username and password despite physical access, in most cases you cannot break in. Certainly some other methods of attack exist so long as you have physical access, but for all intents and purposes in this discussion, the typical, aspiring hacker is locked out. This assists in implementing the more stringent rule set as required by edge and remote access.

In a wireless environment, the rules change. How do you stop access to RF? RF travels through, around, and is reflected off objects, walls, and other physical barriers. RF doesn't have the feature-rich security support that the typical wired network has. Even though you can use the features of the wired Ethernet/IP security model after you are connected to the LAN, what about the signal from the AP to the client and vice-versa? Because of this access methodology, wireless poses some interesting policy challenges.

You can overcome one of these challenges—ease of capture of RF traffic—by preventing the broadcast of the Secure Set Identifier (SSID) to the world from the AP. Much like the Network Basic Input/Output System (NETBIOS) in the Windows world that broadcasts shares, the AP typically broadcasts the SSID to allow clients to associate. This is an advertisement for access to what you would like to be a restricted WLAN. Therefore, a good policy in the WLAN space is to prevent the AP from broadcasting this information. Instead, set up the AP to respond only to clients that already have the required details surrounding the Basic Service Set (BSS). This means that when the client attempts to associate, the AP challenges the client for the SSID and WEP encryption key information before allowing access. Of course, there are still ways to capture the traffic, but

with this minor policy rule, the level of difficulty has been exponentially increased from the default implementation.

This security policy works well in the WLAN space until a technically savvy, but security ignorant, user installs a rogue AP because they wish to have their own personal AP connected to the WLAN. This poses a strong threat to the overall network security posture and must be prohibited.

What's in a name? It's imperative that you set in place a standard naming convention and WEP policy to prevent the standard defaults from being utilized. You wouldn't want your password published to the world in a set of instructions on how to access your PC, but that is exactly the case when speaking of WLAN defaults. They are published, documented, and presented as the default settings of the wireless space built from that specific hardware, and this is a *good* thing. Without this information, you would not be able to implement the hardware. However, to prevent unauthorized access, it's critical that you do not leave the default settings in place. A further consideration would be not using easily guessed names such as the company name. This should be part of your security policy for new hardware/software integration and goes toward assisting in the mitigation of capturing RF traffic.

With respect to roaming needs, these policies should not change from room to room or AP to AP. A consistent rule set (more stringent than normally internally trusted users) should be put in place across all APs where users are likely to roam while connected wirelessly. When choosing your AP, you can also add to ease of use for your wireless users by getting hardware that supports true roaming as opposed to having to lose connectivity momentarily while re-associating with another AP. The temporary loss of connectivity could lead to account lock out and the need to re-authenticate in upper layers.

Finally, strong authentication and encryption methods makes attacking the access mechanisms even more difficult, which is why the organization must include the appropriate use of authentication and encryption in its policy. Use of RADIUS or VPN solutions for authentication and tunneling sits nicely in the gap for the added protection. These authentication tools even serve as a standalone security feature for open networks where disabling the SSID is not an option.

All in all, policy should reflect these general guidelines if you intend to secure the WLAN access to corporate assets. We explore each in detail throughout this chapter to give you the information you need to secure your WLAN. Don't make the mistake of using just one of these options. Instead, look at your security policy as a tightly bound rope consisting of multiple threads. Each thread is another layer of security. In this case, your security policy will remain strong

despite the failure of one or two threads. At no time do you want one solution to be the only boundary between maintaining your valuables and losing them.

Implementing WEP

Despite its critics, WEP still offers a reasonable level of security, providing that all its features are used properly. This means greater care in key management, avoiding default options, and making sure adequate encryption is enabled at every opportunity.

Proposed improvements in the standard should overcome many of the limitations of the original security options, and should make WEP more appealing as a security solution. Additionally, as WLAN technology gains popularity, and users clamor for functionality, both the standards committees as well as the hardware vendors will offer improvements. This means that you should make sure to keep abreast of vendor-related software fixes and changes that improve the overall security posture of your WLAN.

Most APs advertise that they support WEP in at least 40-bit encryption, but often the 128-bit option is also supported. For corporate networks, 128-bit encryption–capable devices should be considered as a minimum. With data security enabled in a closed network, the settings on the client for the SSID and the encryption keys have to match the AP when attempting to associate with the network, or it will fail. In the next few paragraphs, we discuss WEP as it relates to the functionality of the standard, including a standard definition of WEP, the privacy created, and the authentication.

Defining WEP

802.11, as a standard, covers the communication between WLAN components. RF poses challenges to privacy in that it travels through and around physical objects. As part of the goals of the communication, a mechanism needed to be implemented to protect the privacy of the individual transmissions that in some way mirrored the privacy found on the wired LAN. Wireless Equivalency Privacy is the mechanism created in the standard as a solution that addresses this goal. Because WEP utilizes a cryptographic security countermeasure for the fulfillment of its stated goal of privacy, it has the added benefit of becoming an authentication mechanism. This benefit is realized through a shared key authentication that allows the encryption and decryption of the wireless transmissions. Many keys can be defined on an AP or a client, and they can be rotated to add complexity for a higher security standard for your WLAN policy. This is a must!

WEP was never intended to be the absolute authority in security. Instead, the driving force was privacy. In cases that require high degrees of security, you should utilize other mechanisms, such as authentication, access control, password protection, and virtual private networks.

Creating Privacy with WEP

Let's look at how WEP creates a degree of privacy on the WLAN. WEP comes in several implementations: no encryption, and 40-bit and 128-bit encryption. Obviously, no encryption means no privacy. Transmissions are sent in the clear, and they can be viewed by any wireless sniffing application that has access to the RF propagated in the WLAN. In the case of the 40- and 128-bit varieties (just as with password length), the greater the number of characters (bits), the stronger the encryption. The initial configuration of the AP will include the setup of the shared key. This shared key can be in the form of either alphanumeric, or hexadecimal strings, and is matched on the client.

WEP uses the RC4 encryption algorithm, a stream cipher developed by noted cryptographer Ron Rivest (the "r" in RSA). Both the sender and receiver use the stream cipher to create identical pseudorandom strings from a known shared key. The process entails the sender to logically XOR the plaintext transmission with the stream cipher to produce the ciphertext. The receiver takes the shared key and identical stream and reverses the process to gain the plaintext transmission.

A 24-bit initialization vector (IV) is used to create the identical cipher streams. The IV is produced by the sender, and is included in the transmission of each frame. A new IV is used for each frame to prevent the reuse of the key weakening the encryption. This means that for each string generated, a different value for the RC4 key will be used. Although a secure policy, consideration of the components of WEP bear out one of the flaws in WEP. Because the 24-bit space is so small with respect to the potential set of IVs, in a short period of time, all keys are eventually reused. Unfortunately, this weakness is the same for both the 40- and 128-bit encryption levels.

To protect against some rudimentary attacks that insert known text into the stream to attempt to reveal the key stream, WEP incorporates a checksum in each frame. Any frame not found to be valid through the checksum is discarded. All in all this sounds secure, but WEP has well-documented flaws, which we cover in later sections. Let's review the process in a little more detail to gain a better understanding of the behind-the-scenes activities that are largely the first line of defense in WLAN security.

The WEP Authentication Process

Shared key authentication is a four-step process that begins when the AP receives the validated request for association. After the AP receives the request, a series of management frames are transmitted between the stations to produce the authentication. This includes the use of the cryptographic mechanisms employed by WEP as a validation.

Strictly with respect to WEP, in the authorization phase, the four steps break down in the following manner:

1. The requestor (the client) sends a request for association.
2. The authenticator (the AP) receives the request, and responds by producing a random challenge text and transmitting it back to the requestor.
3. The requestor receives the transmission, ciphers the challenge with the shared key stream, and returns it.
4. The authenticator decrypts the challenge text and compares the values against the original. If they match, the requestor is authenticated. On the other hand, if the requestor doesn't have the shared key, the cipher stream cannot be reproduced, therefore the plaintext cannot be discovered, and theoretically, the transmission is secured.

WEP Benefits and Advantages

WEP provides some security and privacy in transmissions to prevent curious or casual browsers from viewing the contents of the transmissions held between the AP and the clients. In order to gain access, the degree of sophistication of the intruder has to improve, and specific intent to gain access is required. Let's view some of the other benefits of implementing WEP:

- All messages are encrypted using a checksum to provide some degree of tamper resistance.
- Privacy is maintained via the encryption. If you do not have the key, you can't decrypt the message.
- WEP is extremely easy to implement. Set the encryption key on the AP, repeat the process on each client, and voilà! You're done!
- WEP provides a very basic level of security for WLAN applications.

- WEP keys are user definable and unlimited. You do not have to use predefined keys, and you can and should change them often.

WEP Disadvantages

As with any standard or protocol, WEP has some inherent disadvantages. The focus of security is to allow a balance of access and control while juggling the advantages and disadvantages of each implemented countermeasure for security gaps. The following are some of the disadvantages of WEP:

- The RC4 encryption algorithm is a known stream cipher. This means it takes a finite key and attempts to make an infinite pseudorandom key stream in order to generate the encryption.
- Once you alter the key—which you should do often—you have to tell everyone so they can adjust their settings. The more people you tell, the more public the information becomes.
- Used on its own, WEP does not provide adequate WLAN security.
- WEP has to be implemented on every client as well as every AP to be effective.

The Security Implications of Using WEP

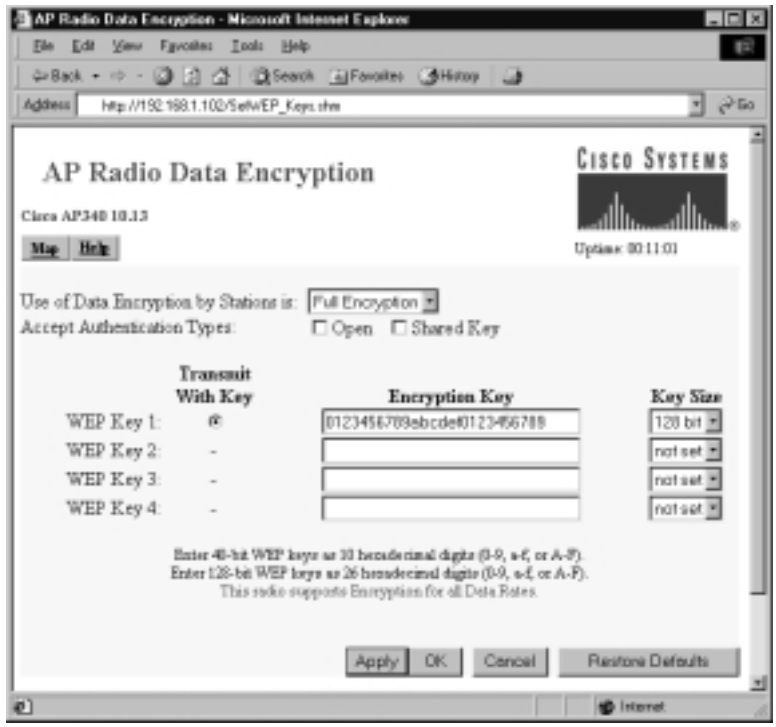
From a security perspective, you have mitigated the curious hacker who lacks the means or desire to really hack your network. If you have enabled WEP as instructed in the previous pages, someone has to be actively attempting to break into your network in order to be successful. If that is the case, using the strongest form of WEP available is important. Because WEP relies on a known stream cipher, it is vulnerable to certain attacks. By no means is it the final authority and should not be the only security countermeasure in place to protect your network—and ultimately your job!

Implementing WEP on the Cisco Aironet AP 340

As you can see in the following, the Cisco AP340 supports 128-bit encryption. It is configured with either a HTTP connection pictured here, or a serial connection. The serial interface is cryptic and in no way intuitive. If you plan on administering many Cisco wireless devices, use the Web interface. In Figure 8.7, you see the Web interface for an AP340. By using the drop-down menu, you can select

Full Encryption and then **128 bit** for the key size. Finally, select the **WEP Key** radio button for the transmission key and type the string.

Figure 8.7 WEP Configuration on the Aironet



Exploiting WEP

There have been a number of well-publicized exploitations and defeats of the security mechanisms at the heart of WEP, from weaknesses in the encryption algorithm to weaknesses in key management. Although steps have been taken to overcome these weaknesses, attackers are not suffering from a lack of networks to exploit.

The first warnings regarding WEP's vulnerability to compromise came in the fall of 2000 when Jesse Walker published a document called "Unsafe at any Size: An Analysis of the WEP Encryption." In this document, Walker underscored the main weakness of WEP—the fact that it reinitializes the encrypted data stream every time an Ethernet collision occurs. Even though the 802.11 protocol attempts to avoid them with CDMA/CA, collisions are a reality that will occur. If someone is listening in on the wireless conversation, they capture the IV information transmitted with each frame and in a matter of hours have all the data needed to recover the WEP key.

Although many experts have made similar discoveries regarding this and other ways to recover WEP keys, these were usually academic and only showed that the potential for vulnerability existed. This all changed with the introduction of AirSnort and WEPCrack. Both of these programs saw an initial release in the summer of 2001, and moved the recovery of WEP keys from being a theoretical to something anyone could do—if they had a wireless card based on the Prism2 chipset.

Security of 64-Bit versus 128-Bit Keys

It might seem obvious to a nontechnical person that something protected with a 128-bit encryption scheme would be more secure than something protected with a 64-bit encryption scheme. This, however, is not the case with WEP. Because the same vulnerability exists with both encryption levels, they can be equally broken within similar time limits.

With 64-bit WEP, the network administrator specifies a 40-bit key—typically ten hexadecimal digits (0–9, a–f, or A–F). A 24-bit IV is appended to this 40-bit key, and the RC4 key scheme is built from these 64-bits of data. This same process is followed in the 128-bit scheme. The Administrator specifies a 104-bit key—this time 26 hexadecimal digits (0-9, a-f, or A-F). The 24-bit IV is added to the beginning of the key, and the RC4 key schedule is built.

As you can see, because the vulnerability comes from capturing predictably weak IVs, the size of the original key would not make a significant difference in the security of the encryption. This is due to the relatively small number of total IVs possible under the current WEP specification. Currently, there are a total of 2^{24} possible IV keys. You can see that if the WEP key was not changed within a strictly-defined period of time, all possible IV combinations could be heard off of a 802.11b connection, captured, and made available for cracking within a short period of time. This is a flaw in the design of WEP, and bears no correlation to whether the wireless client is using 64-bit WEP or 128-bit WEP.

Acquiring a WEP Key

As mentioned previously, programs exist that allow an authenticated and/or unassociated device within the listening area of the AP to capture and recover the WEP key. Depending on the speed of the machine listening to the wireless conversations, the number of wireless hosts transmitting on the WLAN, and the number of IV retransmissions due to 802.11 frame collisions, the WEP key could be cracked as quickly as a couple of hours. Obviously, if an attacker attempts to

listen to a WEP-protected network when there was very little network traffic, it would take much longer to be able to get the data necessary to crack WEP.

Armed with a valid WEP key, an intruder can now successfully negotiate association with an AP, and gain entry onto the target network. Unless other mechanisms like MAC filtering are in place, this intruder is now able to roam across the network and potentially break into servers or other machines on the network. If MAC filtering is occurring, another procedure must be attempted to get around this. This was covered earlier in the "MAC Filtering" section.

WARNING

Because WEP key retrieval is now possible by casual attackers, keeping the same static WEP key in a production role for an extended period of time does not make sense. If your WEP key is static, it could be published into the underground by a hacker and still be used in a production WLAN six months to a year later.

One of the easiest ways to mitigate the risk of WEP key compromise is to regularly change the WEP key your APs and clients use. Although this may be an easy task for small WLANs, the task becomes extremely daunting when you have dozens of APs and hundreds of clients to manually rekey.

Both Cisco and Funk Software have released Access Control servers that implement rapid WEP rekeying on both APs as well as the end-user client. Utilizing this form of software, even if a WEP key was to be discovered, you could rest assured that within a specified period of time, that particular key would no longer be valid.

Addressing Common Risks and Threats

The advent of wireless networks has not created new legions of attackers. Many attackers will utilize the same attacks for the same objectives they used in wired networks. If you do not protect your wireless infrastructure with proven tools and techniques, and do not have established standards and policies that identify proper deployment and security methodology, you will find that the integrity of your wireless networks may be threatened.

Finding a Target

Utilizing new tools created for wireless networks and thousands of existing identification and attack techniques and utilities, attackers of wireless networks have many avenues to your network. The first step to attacking a wireless network involves finding a network to attack. The first popular software to identify wireless networks was NetStumbler (www.netstumbler.org). NetStumbler is a Windows application that listens for information, such as the SSID, being broadcast from APs that have not disabled the broadcast feature. When it finds a network, it notifies the person running the scan and adds it to the list of found networks.

As people began to drive around their towns and cities looking for wireless networks, NetStumbler added features such as pulling coordinates from Global Positioning System (GPS) satellites and plotting that information on mapping software. This method of finding networks is very reminiscent of a way hackers would find computers when they had only modems to communicate. They would run programs designed to search through all possible phone numbers and call each one looking for a modem to answer the call. This type of scan was typically referred to as *war dialing*; driving around looking for wireless networks has come to be known as *war driving*.

NetStumbler.org created place that people can upload the output of their war drives for inclusion in a database that can graph the location of wireless networks that have been found (www.netstumbler.org/nation.php). See Figure 8.8 for output of discovered and uploaded wireless networks as of January 2002.

Similar tools soon became available for Linux and other UNIX-based operating systems, which contained many additional utilities hackers use to attack hosts and networks once access is found. A quick search on www.freshmeat.net or www.packetstormsecurity.com for "802.11" will reveal several network identification tools as well as tools to configure and monitor wireless network connections.

Finding Weaknesses in a Target

If a network is found without encryption enabled, which reports are showing to be more than half of the networks found so far, the attacker has complete access to any resource the wireless network is connected to. They can scan and attack any machines local to the network, or launch attacks on remote hosts without any fear of reprisal, as the world thinks the attack is coming from the owner of the wireless network.

If the network is found with WEP enabled, the attacker will need to identify several items to reduce the time it will take to get onto the wireless network.

First, utilizing the output of NetStumbler or one of the other network discovery tools, the attacker will identify the SSID, network, MAC address, and any other packets that might be transmitted in cleartext. Generally, NetStumbler results include vendor information, which an attacker can use to determine which default keys to attempt on the wireless network.

Figure 8.8 Networks Discovered with NetStumbler (as of January 2002)

If the vendor information has been changed or is unavailable, the attacker can still use the SSID and network name and address to identify the vendor or owner of the equipment (many people use the same network name as the password, or use the company initials or street address as their password). If the SSID and network name and address has been changed from the default setting, a final network-based attempt could be to use the MAC address to identify the manufacturer.

If none of these options work, there is still the possibility of a physical review. Many public areas are participating in the wireless revolution. An observant attacker will be able to use physical and wireless identification techniques—such as finding antennas, APs, and other wireless devices that are easily identified by the manufacturer's casing and logo.

Exploiting Those Weaknesses

A well-configured wireless AP will not stop a determined attacker. Even if the network name and SSID are changed and the secret key is manually reconfigured on all workstations on a somewhat regular basis, the attacker will still take other avenues to compromise the network.

If easy access is available near to the wireless network, such as a parking lot or garage next to the building being attacked, the only thing an attacker needs is patience and AirSnort or WEPCrack. When these applications have captured enough "weak" packets (IV collisions, for example) they are able to determine the secret key currently in use on the network. Quick tests have shown that an average home network can be cracked in an overnight session. This means that to ensure your network protection, you would need to change your WEP key at least two times per day, or keep your eyes open for any vehicles that look suspicious (with an antenna sticking out the window, for instance) parked outside your home or business for hours or days at a time.

If none of these network tools help in determining which default configurations to try, the next step is to scan the traffic for any cleartext information that might be available. Some manufacturers, such as Lucent, have been known to broadcast the SSID in cleartext even when WEP and closed network options are enabled. Using tools such as Ethereal (www.ethereal.com) and TCPDump (www.tcpdump.org) allow the attacker to sniff traffic and analyze it for any cleartext hints they may find.

As a last option, the attacker will go directly after your equipment or install their own. The number of laptops or accessories stolen from travelers is rising each year. At one time these thefts were perpetrated by criminals simply looking to sell the equipment, but as criminals become more savvy, they are also after the information contained within the machines. Once you have access to the equipment, you are able to determine what valid MAC addresses can access the network, what the network SSID is, and what secret keys are to be used.

An attacker does not need to become a burglar in order to acquire this information. A skilled attacker will utilize new and specially designed malware and network tricks to determine the information needed to access your wireless network. A well-scripted Visual Basic script that could arrive in e-mail (targeted spam) or through an infected Web site can extract the information from the user's machine and upload it to the attacker.

With the size of computers so small today (note the products at www.mynix.com/espace/index.html and www.citydesk.pt/produto_ezgo.htm), it wouldn't

take much for the attacker to simply create a small AP of their own that could be attached to your building or office and look just like another telephone box. Such a device, if placed properly, will attract much less attention than someone camping in a car or van in your parking lot.

Sniffing, Interception, and Eavesdropping

Originally conceived as a legitimate network and traffic analysis tool, sniffing remains one of the most effective techniques in attacking a wireless network, whether it's to map the network as part of a target reconnaissance, to grab passwords, or to capture unencrypted data.

Defining Sniffing

Sniffing is the electronic form of eavesdropping on the communications that computers have across networks. In the original networks deployed, the equipment tying machines together allowed every machine on the network to see the traffic of others. These repeaters and hubs, while very successful for getting machines connected, allowed an attacker easy access to all traffic on the network by only needing to connect to one point to see the entire network's traffic.

Wireless networks function very similar to the original repeaters and hubs. Every communication across the wireless network is viewable to anyone who happens to be listening to the network. In fact, the person listening does not even need to be associated with the network to sniff!

Sample Sniffing Tools

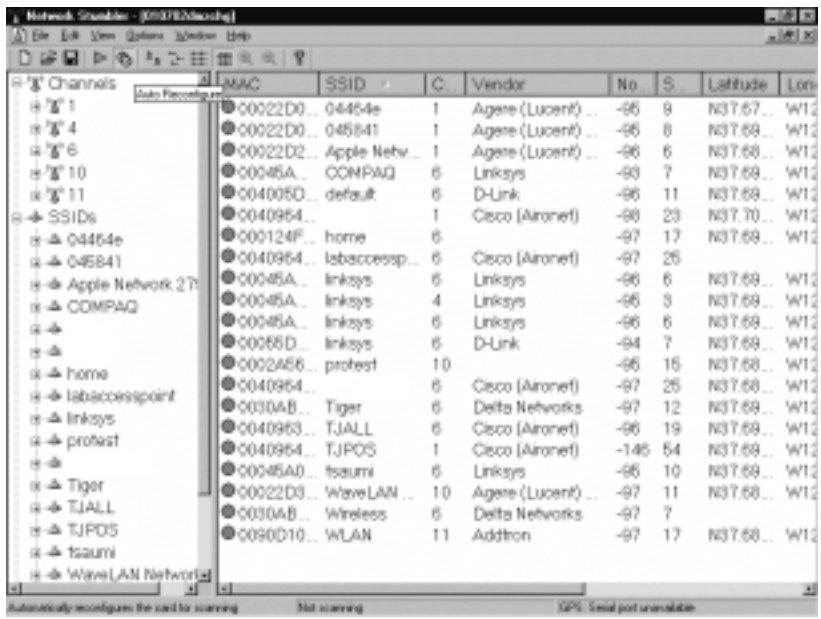
The hacker has many tools available to attack and monitor your wireless network. A few of these tools are Ethereal and AiroPeek (www.wildpackets.com/products/airopeek) in Windows, and TCPDump or ngrep (http://ngrep.sourceforg.net) within a UNIX or Linux environment. These tools work well for sniffing both wired and wireless networks.

All of these software packages function by putting your network card in what is called *promiscuous mode*. When in this mode, every packet that goes past the interface is captured and displayed within the application window. If the attacker is able to acquire your WEP password, they can then utilize features within AiroPeek and Ethereal to decrypt either live or post-capture data.

Sniffing Case Scenario

By running NetStumbler, the hacker will be able to find possible targets. As shown in Figure 8.9, we have found several networks that we could attack.

Figure 8.9 Discovering Wireless LANS with NetStumbler



Once the hacker has found possible networks to attack, one of the first tasks is to identify who the target is. Many organizations are "nice" enough to include their name or address in the network name. For those that do not display that information, we can gather a lot from their traffic that allows us to determine who they could be.

Utilizing any of the mentioned network sniffing tools, the unencrypted network is easily monitored. Figure 8.10 shows our network sniff of the traffic on the wireless network. From this, we are able to determine who their Domain Name System (DNS) server is, and what default search domain and default Web home page they are accessing. With this information, we can easily identify who the target is and determine if they are worth attacking.

If the network is encrypted, the first place to start is locating the physical location of the target. NetStumbler has the capability to display the signal strength of the networks you have discovered (see Figure 8.11). Utilizing this information, the attacker needs to just drive around and look for where the signal strength increases and decreases to determine the home of the wireless network.

Figure 8.10 Sniffing with Ethereal

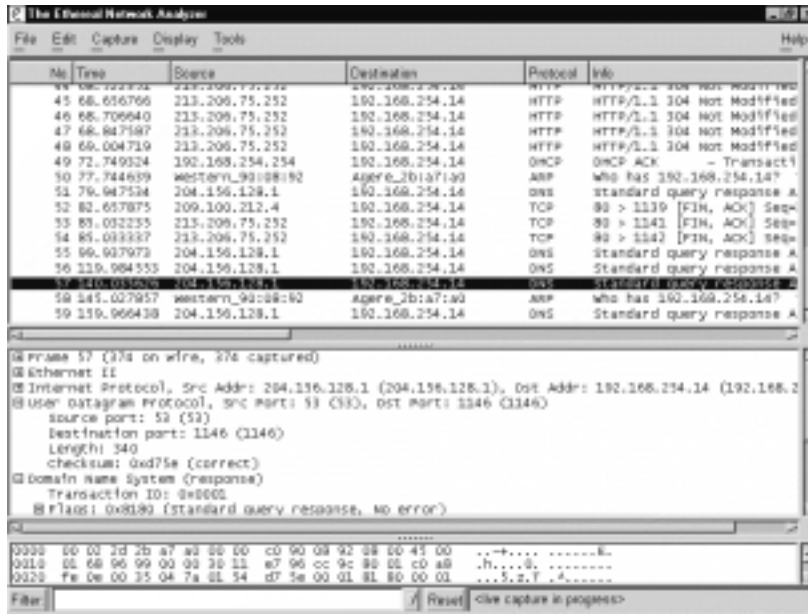
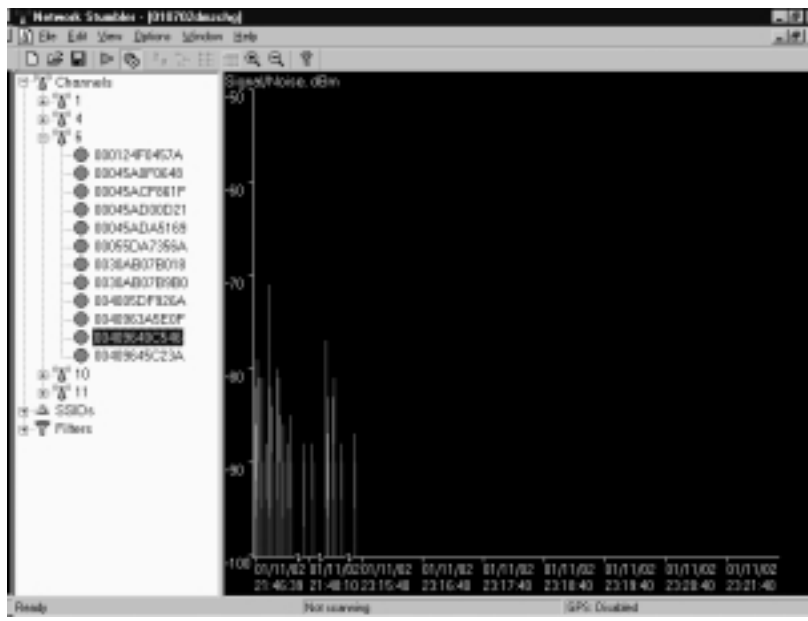


Figure 8.11 Using Signal Strength to Find Wireless Networks



To enhance the ability to triangulate the position of the wireless network, the attacker can utilize directional antennas to focus the wireless interface in a

specific direction. An excellent source for wireless information, including information on the design of directional antennas is the Bay Area Wireless Users Group (www.bawug.org).

Protecting Against Sniffing and Eavesdropping

One protection available to wired networks was the upgrade from repeaters and hubs to a switched environment. These switches would send only the traffic intended over each individual port, making it difficult (although not impossible) to sniff the entire network's traffic. This is not an option for wireless due to the nature of wireless itself.

The only way to protect your wireless users from attackers who might be sniffing is to utilize encrypted sessions wherever possible: Use SSL for e-mail connections, SSH instead of Telnet, and Secure Copy (SCP) instead of FTP.

To protect your network from being discovered with NetStumbler, be sure to turn off any network identification broadcasts, and if possible, close down your network to any unauthorized users. This will prevent tools such as NetStumbler from finding your network to begin with. However, the knowledgeable attacker will know that just because you are not broadcasting your information does not mean that your network can't be found.

All the attacker needs to do is utilize one of the network sniffers to monitor for network activity. Although not as efficient as NetStumbler, it is still a functional way to discover and monitor networks. Even encrypted networks will show traffic to the sniffer, even if you are not broadcasting who you are. Once they have identified your traffic, the attacker will then be able to utilize the same identification techniques to begin an attack on your network.

Spoofing and Unauthorized Access

The combination of weaknesses in WEP, and the nature of wireless transmission, has highlighted the art of *spoofing* as a real threat to wireless network security. Some well publicized weaknesses in user authentication using WEP have made authentication spoofing just one of an equally well tested number of exploits by attackers.

Defining Spoofing

One definition of spoofing is where an attacker is able to trick your network equipment into thinking that the connection they are coming from is one of the valid and allowed machines from its network. Attackers can accomplish this several ways, the easiest of which is to simply redefine the MAC address of your

wireless or network card to be a valid MAC address. This can be accomplished in Windows through a simple Registry edit. Several wireless providers also have an option to define the MAC address for each wireless connection from within the client manager application that is provided with the interface.

There are several reasons that an attacker would spoof your network. If you have closed out your network to only valid interfaces through MAC or IP address filtering, if an attacker is able to determine a valid MAC or IP address, he could then reprogram his interface with that information, allowing him to connect to your network impersonating a valid machine.

IEEE 802.11 networks introduce a new form of spoofing: authentication spoofing. As described in their paper "Intercepting Mobile Communications: The Insecurities of 802.11," the authors identified a way to utilize weaknesses within WEP and the authentication process to spoof authentication into a closed network. The process of authentication, as defined by IEEE 802.11, is a very simple process. In a shared-key configuration, the AP sends out a 128-byte random string in a cleartext message to the workstation wishing to authenticate. The workstation then encrypts the message with the shared key and returns the encrypted message to the AP. If the message matches what the AP is expecting, the workstation is authenticated onto the network and access is allowed.

As described in the paper, if an attacker has knowledge of both the original plaintext and ciphertext messages, it is possible to create a forged encrypted message. By sniffing the wireless network, an attacker is able to accumulate many authentication requests, each of which includes the original plaintext message and the returned ciphertext-encrypted reply. From this, the attacker can easily identify the keystream used to encrypt the response message. She could then use it to forge an authentication message that the AP will accept as a proper authentication.

Sample Spoofing Tools

The wireless hacker does not need many complex tools to succeed in spoofing a MAC address. In many cases, these changes are either features of the wireless manufacturers or easily changed through a Windows Registry modification. Once a valid MAC is identified, the attacker need only reconfigure his device to trick the AP into thinking they are a valid user.

The ability to forge authentication onto a wireless network is a complex process. There are no known "off the shelf" packages available that will provide these services. An attacker will need to either create their own tool or take the time to decrypt the secret key by using AirSnort or WEPCrack.

If the attacker is using Windows 2000, and his network card supports reconfiguring the MAC address, there is another way to reconfigure this information. If your card supports this feature, you can change it from the Control Panel by clicking the **System** icon. Once the System Properties dialog box appears, select the **Hardware** tab and choose **Device Manager**. Within the Device Manager, under the **Network Adaptors**, you should find your interface. If you open the properties to this interface, you should have an **Advanced** tab. Many network adaptors allow you to reconfigure the MAC address of the card from this area.

Now that the hacker is utilizing a valid MAC address, he is able to access any resource available from your wireless network. If you have WEP enabled, the hacker will have to either identify your secret key, or as you will see shortly, capture the key through malware or stealing the user's notebook.

Protecting Against Spoofing and Unauthorized Attacks

Little can be done to prevent these attacks. The best protection involves several additional pieces to the wireless network. Using an external authentication source, such as RADIUS or SecurID, will prevent an unauthorized user from accessing the wireless network and resources it connects with.

If the attacker has reconfigured her machine to use a valid MAC address, little can be done, except the additional external authentication. The only additional protection that you can provide is if you utilize secure connections for all host services accessed by the network. If you use SSH and SSL, you can require valid client certificates to access those resources. Even if a hacker were able to access the network, this would keep her from accessing your critical systems.

However, note that even with this, and without utilizing either a dynamic firewall or RADIUS WEP authentication, an attacker could be able to get onto your network. Even if you protect your critical systems, the attacker will still have access to all workstations on the network, as well as all networks that are connected to the wireless network. She could then compromise those resources and acquire the valid information needed to access your systems.

Network Hijacking and Modification

Numerous techniques are available for an attacker to "hijack" a wireless network or session. And unlike some attacks, network and security administrators may be unable to tell the difference between the hijacker and a legitimate passenger.

Defining Hijacking

Many tools are available to the network hijacker. These tools are based upon basic implementation issues within almost every network device available today. As TCP/IP packets go through switches, routers, and APs, each device looks at the destination IP address and compares it with the IP addresses it knows to be local. If the address is not in the table, the device hands the packet off to its default gateway.

This table is used to coordinate the IP address with what MAC addresses are local to the device. In many situations, this list is a dynamic list that is built up from traffic that is passing through the device and through Address Resolution Protocol (ARP) notifications from new devices joining the network. There is no authentication or verification that the request received by the device is valid. So a malicious user is able to send messages to routing devices and APs stating that their MAC address is associated with a known IP address. From then on, all traffic that goes through that router destined for the hijacked IP address will be handed off to the hacker's machine.

If the attacker spoofs as the default gateway or a specific host on the network, all machines trying to get to the network or the spoofed machine will connect to the attacker's machine instead of where they had intended. If the attacker is clever, he will only use this to identify passwords and other necessary information and route the rest of the traffic to the intended recipient. This way the end user has no idea that this "man-in-the-middle" has intercepted her communications and compromised her passwords and information.

Another clever attack that is possible is through the use of rogue APs. If the attacker is able to put together an AP with enough strength, the end users may not be able to tell which AP is the real one to use. In fact, most will not even know that another is available. Using this, the attacker is able to receive authentication requests and information from the end workstation regarding the secret key and where they are attempting to connect.

These rogue APs can also be used to attempt to break into more tightly configured wireless APs. Utilizing tools such as AirSnort and WEPCrack requires a large amount of data to be able to decrypt the secret key. A hacker sitting in a car in front of your house or office is easily identified, and will generally not have enough time to finish acquiring enough information to break the key. However, if they install a tiny, easily hidden machine, this machine could sit there long enough to break the key and possibly act as an external AP into the wireless network it has hacked.

Sample Hijacking Tools

Attackers who wish to spoof more than their MAC addresses have several tools available. Most of the tools available are for use under a UNIX environment and can be found through a simple search for "ARP Spoof" at http://packetstormsecurity.com. With these tools, the hacker can easily trick all machines on your wireless network into thinking that the hacker's machine is another machine. Through simple sniffing on the network, an attacker can determine which machines are in high use by the workstations on the network. If they then spoof themselves as one of these machines, they could possibly intercept much of the legitimate traffic on the network.

AirSnort and WEPCrack are freely available. And while it would take additional resources to build a rogue AP, these tools will run from any Linux machine.

Hijacking Case Scenario

Now that we have identified the network to be attacked, and spoofed our MAC address to become a valid member of the network, we can gain further information that is not available through simple sniffing. If the network being attacked is using SSH to access their hosts, just stealing a password might be easier than attempting to break into the host using any exploit that might be available.

By just ARP spoofing their connection with the AP to be that of the host they are wishing to steal the passwords from, all wireless users who are attempting to SSH into the host will then connect to the rogue machine. When they attempt to sign on with their password, the attacker is then able to, first, receive their password, and second, pass on the connection to the real end destination. If the attacker does not do the second step, it will increase the likelihood that their attack will be noticed because users will begin to complain that they are unable to connect to the host.

Protection against Network Hijacking and Modification

You can use several different tools to protect your network from IP spoofing with invalid ARP requests. These tools, such as ArpWatch, will notify an administrator when ARP requests are seen, allowing the administrator to take appropriate action to determine if indeed someone is attempting to hack into the network.

Another option is to statically define the MAC/IP address definitions. This will prevent the attacker from being able to redefine this information. However,

due to the management overhead in statically defining all network adaptors' MAC address on every router and AP, this solution is rarely implemented. In fact, many APs do not offer any options to define the ARP table, and it would depend upon the switch or firewall you are using to separate your wireless network from your wired network.

There is no way to identify or prevent any attackers from using passive attacks, such as from AirSnort or WEPCrack, to determine the secret key used in an encrypted wireless network. The best protection available is to change the secret key on a regular basis and add additional authentication mechanisms such as RADIUS or dynamic firewalls to restrict access to your wired network once a user has connected to the wireless network. However, if you have not properly secured every wireless workstation, an attacker need only go after one of the other wireless clients to be able to access the resources available to it.

Denial of Service and Flooding Attacks

The nature of wireless transmission, and especially the use of spread spectrum technology, makes a wireless network especially vulnerable to *denial of service* (DoS) attacks. The equipment needed to launch such an attack is freely available and very affordable. In fact, many homes and offices contain equipment necessary to deny service to their wireless network.

Defining DoS and Flooding

A denial of service occurs when an attacker has engaged most of the resources a host or network has available, rendering it unavailable to legitimate users. One of the original DoS attacks is known as a *ping flood*. A ping flood utilizes misconfigured equipment along with bad "features" within TCP/IP to cause a large number of hosts or devices to send an ICMP echo (ping) to a specified target. When the attack occurs it tends to use much of the resources of both the network connection and the host being attacked. This will then make it very difficult for any end users to access the host for normal business purposes.

In a wireless network, several items can cause a similar disruption of service. Probably the easiest is through a confliction within the wireless spectrum by different devices attempting to use the same frequency. Many new wireless telephones use the same frequency as 802.11 networks. Through either intentional or unintentional uses of this, a simple telephone call could prevent all wireless users from accessing the network.

Another possible attack would be through a massive amount of invalid (or valid) authentication requests. If the AP is tied up with thousands of spoofed authentication attempts, any users attempting to authenticate themselves would have major difficulties in acquiring a valid session.

As you saw earlier, the attacker has many tools available to hijack network connections. If a hacker is able to spoof the machines of a wireless network into thinking that the attackers machine is their default gateway, not only will the attacker be able to intercept all traffic destined to the wired network, but they would also be able to prevent any of the wireless network machines from accessing the wired network. To do this the hacker need only spoof the AP and not forward connections on to the end destination, preventing all wireless users from doing valid wireless activities.

Sample DoS Tools

Not much is needed to create a wireless DoS. In fact, many users create these situations with the equipment found within their homes or offices. In a small apartment building, you could find several APs as well as many wireless telephones. These users could easily create many DoS attacks on their own networks as well as on those of their neighbors.

A hacker wishing to DoS a network with a flood of authentication strings will also need to be a well skilled programmer. Not many tools are available to create this type of attack, but as we have seen in the attempts to crack WEP, much of the programming required does not take much effort or time. In fact, a skilled hacker should be able to create such a tool within a few hours. When done, this simple application, when used with standard wireless equipment, could possibly render your wireless network unusable for the duration of the attack.

Creating a hijacked AP DoS will require additional tools that can be found on many security sites. See the earlier section "Sample Hijacking Tools" for a possible starting point to acquiring some of the ARP spoofing tools needed. These tools are not very complex and are available for almost every computing platform available.

DoS and Flooding Case Scenario

Many apartments and older office buildings do not come prewired for the high-tech networks that many people are using today. To add to the problem, if many individuals are setting up their own wireless networks, without coordinating the installs, many problems can occur that will be difficult to detect.

Only so many frequencies are available to 802.11 networks. In fact, once the frequency is chosen, it does not change until someone manually reconfigures it.

With these problems, it is not hard to imagine the following situation from occurring.

A person goes out and purchases a wireless AP and several network cards for his home network. When he gets home to his apartment and configures his network he is extremely happy with how well wireless actually works. Then all of a sudden none of the machines on the wireless network are able to communicate. After waiting on hold for 45 minutes to get though to tech support for the device, the network magically starts working again so he hangs up.

Later that week the same problem occurs, only this time he decides to wait on hold. While waiting he goes onto his porch and begins discussing his frustration with his neighbor. During the conversation his neighbor's kids come out and say that their wireless network is not working.

So they begin to do a few tests (still waiting on hold, of course). First the man's neighbor turns off his AP (which is generally off unless the kids are online, to "protect" their network). Once this is done the wireless network starts working again. Then they turn on the neighbor's AP again and the network stops working again.

At this point, tech support finally answers and he describes what has happened. The tech-support representative has seen this situation several times and informs the user that he will need to change the frequency used in the device to another channel. He explains that what has happened is that the neighbor's network is utilizing the same channel, causing the two networks to conflict. Once he changes the frequency, everything starts working properly.

Protecting Against DoS and Flooding Attacks

There is little that you can do to protect against DoS attacks. In a wireless environment the attacker does not need to even be in the same building or neighborhood. With a good enough antenna, the attacker is able to send these attacks from a great distance away. There is no indication that there is any reason for the disruption.

This is one of the valid times to use NetStumbler in a nonhacking context. By using NetStumbler, you can identify any other networks that might be conflicting with your network configuration. However, NetStumbler will not identify other DoS attacks or other equipment that is causing conflicts (such as wireless telephones).

Summary

Only through a solid understanding of security fundamentals, principles, and procedures will you be able to fully identify today's security risks. From this understanding, which is built upon "The Big Three" tenets of security (confidentiality, integrity, and availability, or CIA) come the basis for all other security practices. The essential practices usually associated with security build upon the concepts of "The Big Three," which provide tools for actually implementing security into systems. The ability to properly authenticate a user or process, before allowing that user or process access to specific resources, protect the CIA directly. If you are able to clearly identify the authenticated user through electronic non-repudiation techniques usually found in encryption tools such as public-key encryption, you can ensure that the entities attempting to gain access are who they say they are. Finally, if you log the activities performed, a third party can monitor the logs and ensure that all activity happening on a system complies with the policy and standards defined, and that all inappropriate activity is identified, allowing for possible prosecution or investigation into the invalid activity.

Following these practices, through the use of tested and proven identification and evaluation standards, you can fully understand the security risks associated with any object. Once you know the risks, you can provide solutions to diminish these risks as much as possible.

The standard solution is to create a formal security policy along with detailed guidelines and procedures. These guidelines describe the actual implementation steps necessary for any platform to comply with the established security procedure.

By using these standard methods to protect your wireless network, you should be able to develop a clear and concise wireless security plan that incorporates the needs of your organization's highest levels. This plan will allow for the deployment of a wireless network that's as secure as possible and will provide clear exception listings for areas where the risks to your infrastructure cannot be fully controlled.

Through a careful examination of the design of WEP, we identified significant weaknesses in the algorithm. These weaknesses, along with implementation flaws, have lead to the creation of many new tools that can be used to attack wireless networks. These tools allow for the attacker to identify a wireless network through *war driving* and then crack the secret key by passively listening to the encrypted transmissions. Once they have access to the secret key, only those that have deployed additional security measures will have some additional protection for the rest of their infrastructure.

Even if you have a incident response plan and procedure defined in your security standards, if an attack is not known to be happening, there is little you can do to mitigate or rectify the intrusion. The entire discovery and WEP-cracking process is passive and undetectable. Only at the point of attacking other wireless hosts or spoofing their attacking machine as a valid host does the attack becomes noticeable. However, many installations do not implement system logging, nor do they have standards and practices requiring monitoring of those logs for inappropriate activity.

None of these actions will provide protection against one of the oldest attacks known—theft. There is little you can do to protect your resources if critical information, such as network passwords and access definitions, can be acquired by only gaining access to notebooks or backups. High-tech criminals are creating custom malware that can access this information through spam or disguised Web sites.

Although wireless networks are making computing easier and more accessible, understanding the design and implementation weaknesses in 802.11 will help you in preventing attacks. And at times when attacks are unavoidable, by knowing how and where the attackers will come, you may be able to identify when they are attempting to gain access and respond as defined in your standards and incident response practices.

Solutions Fast Track

Understanding Security Fundamentals and Principles of Protection

- ☑ "The Big Three" tenets of security are: *confidentiality*, *integrity*, and *availability*.
- ☑ Requirements needed to implement the principles of protection include proper authentication of authorized users through a system that provides for a clear identification of the users via tested non-repudiation techniques.
- ☑ Internal or external auditors can use logging or system accounting to ensure that the system is functioning and being utilized in accordance to defined standards and policies.

- ☑ Logging can also be the first place to look for evidence should an attack does occur. Ensure that logging is going to a trusted third-party site that cannot be accessed by personnel and resources being logged.
- ☑ These tools are essential to protecting the privacy of customer, partner, or trade secret information.
- ☑ Encryption has provided many tools for the implementation of these security fundamentals.
- ☑ Encryption is not the definitive solution to security problems. For example, a known secret key could be stolen, or one of the parties utilizing encryption could be tricked or forced into performing the activity, which would be seen as a valid cryptographic operation because the system has no knowledge of any collusion involved in the generation of the request.

MAC Filtering

- ☑ Media Access Control (MAC) filtering is effective against casual attackers.
- ☑ MAC filtering can be circumvented by changing the MAC address on the client device.
- ☑ It is difficult to determine if the lack of association is due to MAC filtering or other reasons like an incorrect Wired Equivalent Protocol (WEP) key.

Reviewing the Role of Policy

- ☑ Once basic fundamentals and principles are understood, through the creation of policies and standards an organization or entity is able to clearly define how to design, implement, and monitor their infrastructure securely.
- ☑ Policies must have direct support and sign-in by the executive management of any organization.
- ☑ A properly mitigated risk should reduce the impact of the threat as well as the likelihood that that threat will occur.
- ☑ A clear and well-defined classification and labeling system is key to the identification of resources being protected.

- ☑ Information classification techniques also provide a method by which the items being classified can then have the proper policy or standards placed around them depending on the level or importance, as well as the risk associated with each identified item.
- ☑ Some organizations are required by their own regulations to have clear and well defined standards and policies.

Implementing WEP

- ☑ To protect against some rudimentary attacks that insert known text into the stream to attempt to reveal the key stream, WEP incorporates a check sum in each frame. Any frame not found to be valid through the check sum is discarded.
- ☑ Used on its own, WEP does not provide adequate wireless local area network (WLAN) security.
- ☑ WEP has to be implemented on every client as well as every Access Point (AP) to be effective.
- ☑ WEP keys are user definable and unlimited. You do not have to use predefined keys, and you can and should change them often.
- ☑ Implement the strongest version of WEP available and keep abreast of the latest upgrades to the standards.

Addressing Common Risks and Threats

- ☑ By examining the common threats to both wired and wireless networks, you can see how a solid understanding in the basics of security principles allows you to fully assess the risks associated with using wireless and other technologies.
- ☑ Threats can come from simple design issues, where multiple devices utilize the same setup, or intentional denial of service attacks which can result in the corruption or loss of data.
- ☑ Not all threats are caused by malicious users. They can also be caused by a conflict of similar resources, such as with 802.11b networks and cordless telephones.

- ☑ With wireless networks going beyond the border of your office or home, chances are greater that your actions might be monitored by a third party.
- ☑ Unless your organization has clear and well-defined policies and guidelines, you might find yourself in legal or business situations where your data is either compromised, lost, or disrupted. Without a clear plan of action that identifies what is important in certain scenarios, you will not be able to address situations as they occur.

Sniffing, Interception, and Eavesdropping

- ☑ Electronic eavesdropping, or *sniffing*, is passive and undetectable to intrusion detection devices.
- ☑ Tools to sniff networks are available for Windows (such as Ethereal and AiroPeek) and UNIX (such as tcpdump and ngrep).
- ☑ Sniffing traffic allows attackers to identify additional resources that can be compromised.
- ☑ Even encrypted networks have been shown to disclose vital information in cleartext, such as the network name, that can be received by attackers sniffing the WLAN.
- ☑ Any authentication information that is broadcast can often be simply replayed to services requiring authentication (NT Domain, WEP authentication, and so on) to access resources.
- ☑ The use of virtual private networks, Secure Sockets Layer (SSL), and Secure Shell (SSH) helps protect against wireless interception.

Spoofing and Unauthorized Access

- ☑ Due to the design of Transmission Control Protocol/Internet Protocol (TCP/IP), there is little that you can do to prevent MAC/IP address spoofing.
- ☑ Only through static definition of MAC address tables can you prevent this type of attack. However, due to significant overhead in management, this is rarely implemented.

- ☑ Wireless network authentication can be easily spoofed by simply replaying another node's authentication back to the AP when attempting to connect to the network.
- ☑ Many wireless equipment providers allow for end-users to redefine the MAC address within their cards through the configuration utilities that come with the equipment.
- ☑ External two-factor authentication such as Remote Access Dial-In User Service (RADIUS) or SecurID should be implemented to additionally restrict access requiring strong authentication to access the wireless resources.

Network Hijacking and Modification

- ☑ Due to the design of TCP/IP, some spoof attacks allow for attackers to hijack or take over network connections established for other resources on the wireless network.
- ☑ If an attacker hijacks the AP, all traffic from the wireless network gets routed through the attacker, so they are then able to identify passwords and other information other users are attempting to use on valid network hosts.
- ☑ Many users are easily susceptible to these man-in-the-middle attacks, often entering their authentication information even after receiving many notifications that SSL or other keys are not what they should be.
- ☑ Rogue APs can assist the attacker by allowing remote access from wired or wireless networks.
- ☑ These attacks are often overlooked as just faults in the user's machine, allowing attackers to continue hijacking connections with little fear of being noticed.

Denial of Service and Flooding Attacks

- ☑ Many wireless networks within a small space can easily cause network disruptions and even denial of service (DoS) for valid network users.
- ☑ If an attacker hijacks the AP and does not pass traffic on to the proper destination, all users of the network will be unable to use the network.

- ☑ Flooding the wireless network with transmissions can also prevent other devices from utilizing the resources, making the wireless network inaccessible to valid network users.
- ☑ Wireless attackers can utilize strong and directional antennas to attack the wireless network from a great distance.
- ☑ An attacker who has access to the wired network can flood the wireless AP with more traffic than it can handle, preventing wireless users from accessing the wired network.
- ☑ Many new wireless products utilize the same wireless frequencies as 802.11 networks. A simple cordless telephone could create a DoS situation for the network more easily than any of these other techniques.

Frequently Asked Questions

The following Frequently Asked Questions, answered by the authors of this book, are designed to both measure your understanding of the concepts presented in this chapter and to assist you with real-life implementation of these concepts. To have your questions about this chapter answered by the author, browse to **www.syngress.com/solutions** and click on the **"Ask the Author"** form.

Q: Do I really need to understand the fundamentals of security in order to protect my network?

A: While you are able to utilize the configuration options available to you from your equipment provider, without a solid background in how security is accomplished you will never be able to protect your assets from the unknown threats that will come against your network through either misconfiguration, backdoors provided by the vendor, or new exploits that have not been patched by your vendor.

Q: Am I required by law to have a security policy?

A: If your organization is a video store, deals with children's records, or is associated with the health care or financial industries (and you are located in the United States), you are most likely required by federal regulation to have a defined security policy, and in some cases you are required to have complete third-party audits of your configuration and policies. If you are not required

by legislation, you might still find yourself liable under civil law to provide proper protection for customer or partner information contained within your system.

Q: Is 128-bit WEP more secure than 64-bit WEP?

A: Not really. This is because the WEP vulnerability has more to do with the 24-bit initialization vector than the actual size of the WEP key.

Q: If I am a home user, can I assume that if I use MAC filtering and WEP, that my network is secure?

A: You can make the assumption that your home network is more secure than if it did not utilize these safeguards. However, as shown in this chapter, these methods can be circumvented to allow for intrusion.

Q: Where can I find more information on WEP vulnerabilities?

A: Besides being one of the sources who brought WEP vulnerabilities to light, www.isaac.cs.berkeley.edu has links to other Web sites that cover WEP insecurities.

Q: Can my customers really sue me or my company for being hacked and having their information leaked or misused?

A: In any situation, if you have an established trust with a customer to maintain their information securely and someone breaks into the building or into their corporate servers, a a customer can possibly pursue litigation against you if you did not have any policies or procedures in place to address the risk associated with this and other threats to the customer's information.

Q: If someone can be forced into performing an activity, why should I bother setting up complex security applications?

A: Without those applications in place, you would find that it does not take direct force to attack you or your information. There has always been the possibility that threats could force individuals in key positions to reveal damaging information and secrets, but there is a greater chance that someone will trick a user into disclosing their password or some other security key. Proper training and education are the best defenses in these situations.

Q: I added a firewall to my design. Why should I also need both a policy and external auditing?

A: Again, a firewall may protect you initially, but what do you do as technology changes, or your staff is replaced? Policies and standards ensure that current and future implementations are built in accordance to the definitions laid out by the organization. Adding logging, as well as internal and third-party auditing of the implemented resources helps ensure that the implementations are built in accordance to policy, and that all activity occurring within the environment is in compliance with your standards, guidelines, and policies.

Q: If I have enabled WEP, am I now protected?

A: No. Certain tools can break all WEP keys by simply monitoring the network traffic for generally less than 24 hours.

Q: Is there any solution available besides RADIUS to perform external user and key management?

A: No, plans are available from manufacturers to identify other ways of performing the user/key management, but to date nothing is available.