Chapter 3

Wireless Network Configuration and Security Strategies

Now that I've reviewed some of the theoretical issues related to wireless technologies, I'll move on to examine the practical aspects of setting up a wireless network.

Wireless access points and the client computers that connect to them must be properly configured to operate on a TCP/IP network. Unless a network has specifically been configured otherwise, wireless clients receive their TCP/IP configuration details through DHCP (see Chapter I, p. 11). It would be extremely inconvenient for a network administrator to manually assign IP addresses to wireless clients' computers every time they roam into an organization's network. Although there may be authentication credentials that need to be manually entered, most wireless users won't need to manually set their IP addresses, default gateways, subnet masks, or any of the other TCP/IP configuration details (see Chapter I, "Network Basics").

One prominent exception to this may be networks on which the system administrator needs tight control of each individual device.

Configuring an Access Point

One of the basic steps in setting up a WLAN involves installation and configuration of one or more access points. The procedures for configuring an access point vary from one equipment manufacturer to another. Most access point units have an administrative interface that can be accessed and operated through a Web browser. Other types of access point units are equipped with a software utility that can be accessed and operated from a PC connected to the network. Either way, the process involves assigning the unit its IP address and other TCP/IP settings and then working through all the configuration details.

The configuration process begins with powering the unit and connecting it to an Ethernet connection on the network. Access points with a Web interface then can be accessed through another computer on the same network by typing in the default IP address for the unit as a URL in a Web browser. If all goes well, the unit will respond by prompting for the default password, which should be listed in the access point's user manual.

Administrative password–One of the first tasks should be to change the administrative password from the manufacturer's default password. As with all network equipment, the password should be complex and non-guessable.

TCP/IP configuration–One group of access point settings involves the standard TCP/IP configuration details: IP address, subnet mask, and default gateway. Although it's possible to have the unit request its TCP/IP settings through DHCP, most network administrators prefer to manually assign static addresses to network components and servers.

SSID–One of the basic configuration elements involved in connecting to a WLAN is the "Session Set ID," or SSID, a string of characters used to identify the network. A SSID can be unique to each access point, or it can be common to a group of access points that comprise an organization's WLAN. One cannot connect to a WLAN without knowing its SSID. Learning the SSID for a network is usually trivial, because by default it's broadcast as part of the beacon signal of an access point. When you launch your wireless client utility and it displays a list of wireless networks available, this corresponds to the SSID's broadcasts by any access points in range. The list may also include client computers in ad hoc mode.

While the common practice involves allowing the SSID to be broadcast by an access point, it's possible

to disable this feature. Because it's necessary (but not sufficient) to know the SSID to establish a connection through an access point, suppressing it can be used as an access-control mechanism. With the SSID broadcast suppressed, one must manually enter the SSID as part of the client configuration. Some organizations may give out the SSID only to individuals authorized to use the wireless network and will change it frequently. This "shared secret" approach provides a pragmatic way to limit network access to those authorized, but it cannot be considered an effective security strategy. Those determined to access the network will be able to discover the SSID, usually through non-technical means.

SSID suppression might be used, for example, by a university that wants its wireless network to be used mostly by its enrolled students. The consequences of others getting into the network would not be severe because usernames, passwords, or other authentication credentials would be required to gain access to any systems on the network.

Access points come with an SSID preset to a default value, which is often the name of the company that manufactured the unit. It's good practice to change the SSID to another value during the initial configuration, even if your network consists of only one access point. The default SSIDs are well-known among hackers, who may also know the default administrative password. You should, of course, change the administrative password because not doing so can allow someone to reconfigure it and defeat any security measures put in place.

Channels—As noted in Chapter II, "Wireless Basics," 802.11 makes use of a number of narrow channels within a broader frequency range. 802.11b and 802.11g devices can be set to channels one through fourteen, but within the United States only channels one through eleven are allowed. Access points may be pre-programmed to allow only the channels permitted in the country for which it was sold. To keep with the pragmatic approach of using non-overlapping channels, units usually will be set to channels one, six, or eleven. If your network consists of a single access point, the choice is arbitrary. If you are covering a larger area with multiple access points, then you'll need to develop a map that describes the coverage of each and make channel assignments to ensure adjacent units are set to different channels.

MAC Address Filters—Almost all access points include the ability to control the client computers that will be allowed, according to lists of MAC addresses. MAC addresses, as noted in Chapter I, p. 8, are usually Ethernet addresses associated with network interface cards in computers, PDAs, or other devices and are guaranteed to be unique worldwide.

MAC address filters are optional. Unless explicitly set, access points will accept connections from any device with the correct SSID or security keys. But with a MAC address filter activated, even a computer that presents the correct authentication credentials will not be allowed to connect if its MAC address isn't one of those allowed. MAC address filters can be set to deny implicitly, so that all clients are rejected except those specifically pre-authorized according to their Ethernet addresses. MAC address filters also can be set to accept clients implicitly, so that all clients are allowed unless they have been blacklisted. The latter approach might be used to lock out computers that previously have caused problems on the network.

MAC address filters work well in a small office or home network. In these environments, the number of devices intended to connect to the network is relatively small. It's easy enough to note the Ethernet addresses of all the computers and printers and add them to the allowed list of the access point and deny all others. This will prevent your neighbors and passersby from freeloading Internet access through your wireless network.

Security Configuration—A number of options can be selected to control security and privacy. By default, most access points will *not* have the security features enabled. This means the traffic between the access point and each client computer will be sent without encryption, allowing the possibility for eavesdropping. The security options available will vary, but all models should offer **WEP** (**Wired Equivalency Privacy**). Enabling this security protocol involves creating a security key and selecting the key length.

Newer models will offer **WPA** (**Wi-Fi Protected Access**). WPA relies on a system of constantly changing keys. Ideally, WPA operates in conjunction with an authentication server to make key assignments but can also operate with static pre-shared keys. Even with pre-shared keys, WPA offers much stronger security than WEP. Both WEP and WPA require the network administrator to provide a "passphrase" or security key in hexadecimal format to the network users. To use WPA without pre-shared keys, the configuration of the access point will include providing the IP address and port number of the Radius server and its associated security key. (Wireless security issues will be discussed in more detail, under the "Wireless Security" section in this chapter, beginning on p. 24.)

Eliminating Rogue Access Points

When positioned in an inappropriate security zone, a wireless network can compromise the overall security of an organization's network. To be secure, a wireless LAN must fit within the organization's overall network design and security architecture. Efforts must be made to detect and remove rogue access points or, at least, to bring them within the official network and support system.

It's fairly easy to detect a rogue access point that broadcasts its SSID. Those that don't broadcast their

SSIDs are a bit harder to detect. Detecting these rogue points may require "white-hat" hacking techniques–the capture and analysis of the wireless traffic to detect the presence of network traffic associated with access points outside of the official network.

The presence of rogue access points are often a symptom of an unresponsive IT support group. Departments resort to setting up informal wireless LANs when they see it as easier than waiting for the organization's IT personnel to respond for their connectivity and collaboration needs.

Cost Issues

Wireless networks can be much less expensive to implement than wired networks. When establishing a wireless LAN for public use, the library provides only the basic connectivity. Users bring their own computers, not only saving the library in computer hardware costs, but also in furniture, Ethernet drops, power outlets, plus the building space.

The installation of a wireless network, however, will include several cost components. For large networks, the budget should include the cost of a site survey and consulting services if the organization doesn't have trained network engineers on staff. Other cost components include the access points and the installation of Ethernet drops and power outlets at each location. If your network design requires authentication, implementation of a splash page or a click-through policy page, bandwidth management, or use reports, you will also need to factor in the cost of some of the added-value products described in the following section.

Enterprise Wireless Networks

Large organizations have complex network needs. A network with thousands or tens of thousands of nodes must be built with manageability and reliability in mind. The equipment used in these networks will have components that allow them to be configured, monitored, and managed through a centralized network management console. It's not tenable (in large networks) for the network administrator to have to visit each piece of equipment for troubleshooting or to make configuration changes.

SNMP–The primary protocol underlying this approach is called "Simple Networking Management Protocol," or SNMP. Devices on the network will include an agent that can respond to commands issued by the management console. The management-related components increase each equipment item's cost but help the organization contain the personnel costs to manage the network. This network management scheme also results in high reliability, because many technical problems can be resolved before they present overt symptoms.

WLAN Switch–In response to the needs of managing a large number of access points on an enterprise network, a new category of equipment has been created called the "WLAN Switch." As noted previously, a standard access point contains components related to wireless radio and components related to the implementation of media access control and security protocols (802.3, 802.11a/b/g/i, WEP, WPA, WPA2). As part of the security protocols, the access point must have the ability to encrypt and decrypt data streams–a task that requires intensive processing.

The WLAN switch presents an architecture that involves a slimmed-down access point, consisting mostly of the radio circuitry, which then transfers all the other functions to the WLAN switch device. The raw traffic of the remote radio travels over the wired Ethernet to the WLAN switch for processing. The WLAN switch typically is housed in an equipment rack alongside the Ethernet switches, routers, and other network gear.

A stand-alone access point has a relatively small amount of computing power, but the WLAN switch, like other enterprise-level networking components, is a specialized device with a fast and powerful processor. A single WLAN switch can control many remote radios.

The centralized approach of the WLAN switch offers many capabilities not possible with a network comprised of multiple stand-alone access points. Some of the benefits available in a WLAN switch include the ability to:

- detect a failed remote radio and attempt to reset the device or reconfigure the network so that adjacent radios can provide at least some coverage for the affected area;
- perform more intelligent, proactive roaming, resulting in better performance for users that roam from one zone to another; and
- detect and block rogue access points.

802.1X authentication–Enterprise networks involve large numbers of users that must be authenticated and authorized as they attempt to use the many services available. It wouldn't be reasonable for each individual device or application to maintain its own database of usernames, passwords, credentials, and authorization levels. Large organizations will implement a centralized authentication server that stores this information once and can be queried as needed. An authentication server follows standards established for this function, usually RADIUS (remote authentication dial-in user service) or LDAP (lightweight directory access protocol).

The recent security protocols associated with wireless networking, including WPA and 802.11i, incorporate 802.1X authentication, which involves performing an authentication request through RADIUS or LDAP as part of the user's association with an access point. 802.1X provides an infrastructure for periodically assigning new keys in encrypted data packets, significantly increasing the strength of security.

Although a home or small network office would probably not have the infrastructure in place for 802.1X authentication, it would be expected in an enterprise network.

Wireless Security

From its earliest days, wireless networking has suffered from a bad reputation involving security. True, in its earlier phases, that reputation was well deserved. But today security options are available for wireless networks that rival the security possible on wired networks. In this section, I'll take a look at the issues that make security more of a concern for wireless networks as well as the technologies available to make wireless networks safer for users.

In Chapter 1, "Network Basics," eavesdropping was discussed as the "bane of security." Ethernet's 802.3 CSMA/CD and the 802.11a/b/g CSMA/CA *do not* preclude the possibility that one network station will be able to open and read the packets of its neighbor's station.

This possibility for eavesdropping is very problematic for both security and privacy. From a privacy perspective, it's important to know when eavesdropping parties might be able to compromise one's network communications. It's also important to have options available for having completely private sessions when dealing with sensitive information. From a security point of view, eavesdropping is a major concern because it might enable an intruder to discover the passwords used for computer administration or view, copy, or destroy data stored on the network-connected computers. The classic hacking scenario involves an intruder getting access to a network in such a way that allows the capture of sensitive information.

In the Ethernet discussion in Chapter 1, "Network Basics," I discussed the "rules of normal communication," which allows a station to open network packets with destination addresses matching its own MAC address. It's possible, however, for a station to operate in promiscuous mode and open any and all packets on the network. A network sniffer operates with a network card in promiscuous mode and has software that captures network traffic, sorts it out according to each station on the network, and presents it in human-readable form.

In the hands of a trusted network administrator, a sniffer is a powerful diagnostic tool. It's bad news, however, when an unauthorized intruder wields such a weapon against your network. Unfortunately, these tools are commonplace, and one must operate all networks with the assumption traffic is being monitored by unfriendly forces.

As networks have evolved, though, increasingly they've become less vulnerable to "sniffing." Again, in the Ethernet discussion in Chapter I, it was noted that media is shared by all the devices participating in a segment. In the original coaxial-based Ethernet, a segment included all the devices physically connected to the same length of cable. All the devices plugged into a shared media Ethernet hub constitute a segment; a single port of an Ethernet switch is tantamount to a segment. The movement toward switched Ethernet has dramatically reduced the number of computers exposed to any given eavesdropping attempt.

Consider how an intruder could eavesdrop. On a wired network, eavesdropping occurs when the intruder is able to gain control of one machine on the segment. This could be possible through direct physical access, such as installing software on an unattended computer. Someone also could visit the premises with a laptop equipped with sniffing software and plug into an unattended Ethernet port. More often, it's done through remote hijacking, taking advantage of some un-patched vulnerability in the computer's operating system or one of its applications.

Once in control, the intruder will install a sniffer, hoping to gain access to the more interesting parts of the network. Rather than view all the traffic on the segment, the sniffer could be set up with triggers that begin capturing only when something interesting happens. Some of the more obvious text patterns that could fire a trigger would be "username," "password," "root," "ssn" (social security number), "credit card," and the like.

Encryption to the Rescue

Does this mean that networks are hopelessly insecure? Not at all. All the scenarios described involve networks that pass information around as "clear text." The solution to providing security and privacy on networks is encryption. If applied properly, an encrypted message is encrypted before it's introduced to the network and can only be decrypted by the specific individual or device for which it is intended.

The encryption schemes used today require the use of a key, usually in the form of a long string of characters. This key is used to encrypt the message on the transmitting end and to decrypt it on the receiving end. Challenges involve ensuring the key cannot be discovered by an intruder and providing a working key to the individual or device authorized to open the message. Theoretically, it's possible to use a computer program to break a security key through brute force, but the use of long security keys makes it much more difficult to crack a key in this way. I'll discuss how some of the wireless security protocols deal with encryption next.

Wireless Security Protocols and Encryption

Wireless networks can be even more vulnerable to eavesdropping than wired networks because access to

the network can be gained by proximity (rather than a direct physical contact). It's also more likely that software for network sniffing will be installed and used, given that the intruder supplies the client computer. Unprotected wireless access points can be an easy entry point for mobile intruders.

A classic scenario involves hackers that attempt to penetrate an organization's network via unprotected wireless access points. In the earlier days of wireless networks, it was fairly common for an organization to have wireless networks set up in such a way that left the entire network vulnerable. For instance, so as not to have to wait for an overworked IT staff to add additional network connections, non-IT departments (without the support of IT personnel) often set up rogue WLANs, yielding an informal network with wireless Internet access for the department. These WLANs almost always had the security features disabled and were often positioned in such a way that could provide inappropriate access to the organization's business systems.

War Driving and Warchalking

This proliferation of insecure WLANs led to a type of hacking that came to be known as "War Driving." It worked like this: Someone interested in getting access to a wireless network—either for the purpose of snooping around an organization's internal network or just to freeload Internet access—would build or buy a sensitive directional antenna for his or her laptop and begin searching for hotspots. Tales were told of hackers, sitting in corporation or government agency parking lots, using these directional antennas to probe for and connect to unsecured wireless networks. These high-gain directional antennas could access networks far past their normal range.

Once connected, the hacker in the parking lot could begin sniffing the internal network in search of passwords or other clues that might make it possible to gain access to the organization's sensitive systems and data. This phenomenon came to be called "War Driving," patterned after the "War Dialing" technique featured in the 1983 movie *War Games* that involved rapid-fire dialing of random numbers in search of modem-connected computers.

"War Driving" led to "Warchalking." Once a WLAN was discovered, one of the infiltrators would leave behind physical graffiti that would describe the network—for the benefit of other intruders that also might want to pay an unauthorized "visit." A set of symbols was adopted to show the particular network's characteristics—whether it was completely open, its SSID, the flavor of 802.11 used, and the amount of bandwidth available. These symbols might be chalked on a wall or sidewalk near the building with the hotspot.

The legends of Warchalking, largely, have outlived the underlying concerns. In the early days of wireless LANs, the main reason War Driving was such a concern was related to the informal nature of these rogue hotspots. Not only were these networks set up without even the most basic of security features enabled, but they also were positioned in a way that exposed the organization's internal network.

Today, most corporate, educational, and government network administrators are entirely aware of the security problems rogue access points can bring about, thus, they have implemented reasonable security measures to protect their wired and wireless networks. A "War Driver" would find few wireless networks worth the trouble these days. Hackers who are able to achieve access to internal networks will find that sensitive internal network communications are almost always protected by industrial-strength encryption. Open networks, generally, offer nothing more interesting than free Internet access. And with numerous free and fee-based Wi-Fi hotspots available for Internet access, War Driving—for the purpose of a free ride on the Internet—has declined. This isn't to suggest that wireless networks do not pose security concerns; it just means that there are ample tools and technologies available that permit wireless LANS to coexist safely with sensitive wired networks.

Wireless Security Strategies

There are two fundamental approaches available for wireless security. The first acknowledges the wireless network will be open and insecure and focuses on isolating it from the rest of the network. Alternatively, the second approach contends that a wireless network can be made secure through authentication and encryption.

This first wireless network security approach relies on separation and segregation. The prime directive in this strategy involves making sure that no matter what may happen on the wireless LAN, the rest of the organization's wired network will remain safe. Some network administrators may accomplish this level of separation by making the wireless network physically separate. The WLAN would have its own Internet connection and its own hubs and routers, eliminating any possibility for the wireless network to compromise the wired network.

Logically, a wall of separation can be accomplished too. One could, for example, use separate switch ports for the wireless network and establish a separate VLAN (Virtual Local Area Network) so the wired network's packets are invisible to wireless users, even though users share some physical equipment.

Libraries open to the public face the same type of issue even if they don't have a wireless network. Almost all libraries offer a set of computers for public use. Library patrons use these computers to access the library's online catalog, the electronic resources to which the library subscribes, and for general Internet access.

The library's other computers are used for library operation and may store sensitive information. The network of computers used by library staff most likely contains budget and personal information, patron circulation data—which may include names, addresses, telephone numbers, and even social security numbers. Obviously, it's very important that such information be protected.

A library's public access computers must be approached with great attention to security. In most cases, library patrons use these computers anonymously and without authentication. Although the library may implement an environment that prevents users from installing software, tampering with the system, or even accessing the operating system, these systems are not foolproof and one must operate under the assumption that malicious activity could happen.

To achieve a secure and protected wireless network environment, it's vital the library's public access computers be separated—that they are positioned well away from the staff side of the library network. In order to avoid accidental intermingling with the staff network, it's important the network cabling to public access computers be thoroughly documented. In addition, the public access network should connect to the main network through a separate set of hubs or switch ports. Setting up a separate VLAN for public computing can be a very effective method for isolating its traffic from the staff network.

It's also important to ensure the library's firewall has been configured accordingly. It usually makes sense to place the library's public computing network on the outside of the firewall, or at least within a security zone defined as "untrusted." Many firewall configurations will include a "DMZ" (demilitarized zone) that contains devices within the building that cannot be considered as trusted. Placing the public access computers in a DMZ can be an effective way to isolate them.

The classic security model involves placing a firewall between the organization's LAN and the Internet. This approach may be too simplistic for many networks. In many cases, multiple firewalls may be needed to provide the necessary protection layers.

Often, the strongest firewall will be placed in front of the organization's business systems, which, of course, is necessary. But it's the network's inner core that requires the most aggressive protection. For example, most networks employ a firewall on the network edge as it connects to the Internet, which serves to block traffic known to be unfriendly. Within the network, there will be multiple zones with differing levels of sensitivity and trustworthiness. A library's bank of public workstations represents a zone with low trust that should be walled off from other zones that contain sensitive information and systems.

If a library already has in place a solid security architecture that segregates its public access computers from the traffic of its staff network, then adding a wireless LAN for patron use can be accomplished fairly easily. The WLAN simply can be positioned with the public access network. The solid wall of demarcation that prevents any potential attack from the public network to the staff network will also serve to isolate the wireless network. If, however, the library has not implemented an adequate security strategy for its public computers, then it has considerable work to do to shore up that front, much less add a WLAN to the mix.

Is It Safe to Have an Open WLAN?

One of the security imperatives in a wireless LAN set-up is to ensure the WLAN cannot harm your library's internal network. One of the key factors to consider in setting up a WLAN involves whether or not to enable security options. With security disabled, users will be able to connect without being given a security key or pass phrase, and their communications will be sent in clear text over the wireless network. Most of the Wi-Fi hotspots available to the public operate with no encryption security. Many hotels, airports, coffee shops, libraries, and other venues offer wireless hotspots to the public, either as a complimentary service or for a fee. Such wireless access has become a basic expectation when traveling.

From the hotspot-hosting establishment's perspective, the prime concern is that no harm comes to the *hosting establishment's* computer systems. Commercial wireless services exist completely separately from the business networks of the establishments in which they reside. Most wireless services are offered through national companies (such as T-Mobile and ICOA) that specialize in the deployment of wireless Internet services in business settings.

With all the concern about wireless security, why don't these public services offer encryption? Is it safe to use an unencrypted wireless service?

It's important to remember that wireless networks must *balance* convenience and security. All the security protocols that offer encryption require the distribution of security keys. When serving the general public, key distribution can be difficult.

Let's consider the vulnerabilities of an open wireless network. As discussed earlier, eavesdropping is a major issue. If you access an open WLAN, you have to assume your traffic can be monitored. That's an assumption you need to make anytime you connect to the Internet. Your computer may be visible to other users of the hotspot. Some of the precautions to take include:

- if you have any shared folders on your computer, require a username and password;
- install and enable a personal firewall on your computer. Windows XP now includes an integrated

personal firewall. A popular option is ZoneAlarm; and

- install and activate anti-virus software, and make sure its virus signature file is updated frequently.

Most importantly, use precaution when dealing with any sensitive information on an open wireless network. Do not—without the use of encryption—transmit credit card numbers, usernames and passwords to sensitive computer accounts, bank account numbers, or any other information that, in the wrong hands, could lead to financial loss, identity theft, or embarrassment. For Web-based applications, make sure the SSL (secure sockets layer) is enabled by the system involved. A locked padlock icon, displayed on a Web browser's status line, indicates you're protected by an encrypted session.

If your laptop contains sensitive information, you need to be extremely careful when using an open wireless connection. Those who travel with classified information, sensitive corporate data, or customer's financial files, for example, would not want to connect to an insecure network of any type, much less an open wireless LAN.

These guidelines are not that different from any other time you connect to the Internet, but access through an open wireless connection is especially vulnerable. Given these caveats, it's reasonably safe to make use of a public, non-encrypted wireless network for Web browsing, routine e-mail, and other non-sensitive activities.

Open wireless networks put the burden of security on the user. Whether you use your mobile computer on the wireless network in your home, at Starbucks, or in your local public library, the same risks apply. If you operate a public wireless service, should you bear the responsibility for educating its users of the risks? Opinions vary, but many services enforce a click-through agreement waiving liability.

A Security/Privacy Must: Encryption

Given the possibility for eavesdropping on networks, sending sensitive information across any network isn't safe without encrypting it. From their earliest versions, wireless networks have included encryption schemes to help make them secure. As wireless LAN technology has evolved through several generations of security architecture, the technology has improved, with each generation yielding more effective security than the last.

Wired Equivalency Privacy (WEP)—From their earliest days, wireless LANs have been designed to include security protocols available to encrypt the traffic between the access point and each client computer. The first version of a wireless LAN security protocol was deemed "WEP," or Wired Equivalency Privacy. The name suggested, with it enabled, the wireless network offered the same amount of privacy (or protection from eavesdropping) as did wired networks.

WEP remains an optional security feature. Most wireless equipment comes with it disabled by default. A wireless access point will transmit its traffic in the clear unless one of the available security protocols is enabled and the security and authentication credentials are distributed to its authorized users.

To enable WEP, one uses the administrative interface of the access point. Usually the process is as simple as selecting the security tab, selecting WEP as the security mode, and proving a security key, generated by typing in a pass phrase. Once the settings are saved and applied, a user won't be able to connect to the access point until the individual provides the correct security key. Because one must provide the specific key assigned with the access point, WEP requires that the network administrator distribute the key to authorized users. To maintain effective security, the distribution must be done in a way that keeps it private. Writing down the key in a public place, for example, probably would not be recommended. With WEP, keys must be changed manually, and there is no automatic mechanism for key distribution. In addition, WEP keys are static; they should be changed periodically so if an unauthorized individual discovers a key, it will only be useful until the next time the key is changed.

In operation, WEP combines its static key with a 24-bit initialization vector (IV) to seed the RC4 algorithm that encrypts the data, or payload, to be transmitted. To decipher the payload, the receiving station needs to know both the static key, which has already been provided to it, and the IV for each packet. The IV is transmitted in the packet headers, outside the encrypted payload. WEP also makes use of a 32-bit integrity check value, a checksum that verifies the data packet hasn't been tampered with during transmission.

Unfortunately, WEP can be cracked easily. The relatively short keys, the use of a single static key, and the lack of a key management system result in a weak security environment. It was quickly discovered that by capturing a relatively small volume of raw data from transmissions on a wireless network, the WEP key could be recovered through brute force algorithms. Readily available Open Source programs, such as WEPCrack and AirSnort, effectively reveal the WEP keys, providing an operator with the means to connect to the WLAN.

Although the WEP protocol can be compromised, it doesn't necessarily mean it shouldn't be enabled. If you're not dealing with top-secret information and want some reasonable degree of security on your network, WEP may be adequate. Most of us lock our homes and cars knowing that anyone who is determined enough can break in. And although WEP can be defeated by a knowledgeable and persistent intruder, it provides a moderate barrier that prevents most unwanted freeloading or intrusions.

802.11i: The Next Generation of Wireless Security

In order to be accepted in business environments with rigorous security requirements, wireless networks need something much stronger than WEP. The development of 802.11i, which specifies a security framework for wireless LANs, is a response to the inadequacies of WEP.

This security framework describes a number of security components that address the weaknesses present in WEP. Some portions of 802.11i were adopted prior to its ratification in June 2004. Even today, products that support all aspects of 802.11i are not widely available.

Wi-Fi Protected Access (WPA)–The first phase of security improvements for wireless LANs came in the form of WPA, or Wi-Fi Protected Access. WPA offers a security environment without the flaws evidenced in WEP. WPA specifies a key length of 128 bits, a key length far more difficult to break.

One of the WPA characteristics involves Temporal Key Integrity Protocol, or TKIP. Besides using easily decoded (too short) keys, one of the problems with WEP is due to its use of keys that never change. WPA addresses this issue through a scheme that uses unique base keys for each session of each client and changes them periodically during the session. Like WEP, WPA uses a combination of the secret key with initialization vector, but the IV is longer (48 bits).

Another WEP weakness involves the lack of effective key management. WPA supports the 802.1X for authentication and key management. 802.1X provides a framework for enforcing authentication, and the framework involves three participants:

- *Authenticator*: a device that requires authentication before use;
- *Supplicant*: a device requesting use of the authenticator; and an
- *Authentication Server*: a server with a database of all the network users and their authentication credentials. Most authentication servers will use RADIUS or LDAP.

This conversation among the Authenticator, Supplicant, and Authentication Server takes place through a language called Extensible Authentication Protocol (EAP). If an access point is configured to require 802.1X, it will use EAP to authenticate clients before granting access. When a client (Supplicant) attempts to associate with the access point (Authenticator), the access point initially will allow only network traffic related to EAP, and it will relay a request from the client to an LDAP or RADIUS server (Authentication Server). If the authentication succeeds, the access point then will allow the client to engage in regular communications. The authentication server also will be used to distribute dynamically generated security keys to the client, and the server will periodically refresh them. 802.1X works well in organizations that already have an infrastructure that includes LDAP or RADIUS. For those that don't, WPA supports the use of pre-shared keys, allowing a secret key to be manually distributed to each authorized client. Although not as secure as using 802.1X, WPA with pre-shared keys is much more secure than WEP.

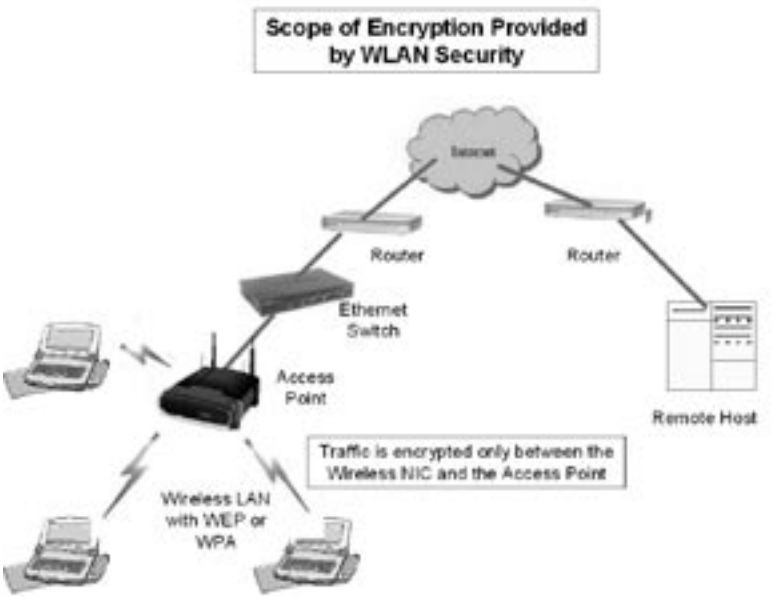

Figure 8
Illustration of the scope of security provided by WLAN security.

WPA was promoted by the Wi-Fi Alliance, an industry consortium concerned with the promotion and interoperability of wireless networking products. Prior to the ratification of the full 802.11i, WPA was presented as a way to deploy secure wireless networks without having to replace all the existing hardware. In most cases, equipment manufactured to support WEP could support WPA by only upgrading software or firmware.

Today, as WEP declines, WPA is gaining wide use. Most access points and clients of recent vintage support WPA. The wireless networking built into Windows XP supports WPA, available in a patch released in March 2003. Apple included support for WPA beginning with AirPort 3.2, which was released in October 2003.

WPA2–Now that the 802.11i security framework has been ratified,

it's been dubbed as "WPA2" by the Wi-Fi Alliance. One optional component of WPA2 that results in higher security involves the use of the Advanced Encryption Standard (AES), which is much stronger than TKIP. While WPA2 is compatible with WPA, it is incompatible with WEP. Implementing WPA2 may require a hardware upgrade. Also, AES requires more processing capabilities that may not be present on older units. WPA2 continues to offer a "lite" version for the home and small office that lacks 802.1X authentication infrastructure. Pre-shared keys continue to be an option, too. The use of the full 802.11i security framework with 802.1X authentication and AES results in a wireless network that not only finally delivers wired equivalency privacy, but may also surpass the security available on most wired networks.

Wi-Fi Security Services—If you want to take advantage of the full suite of security services available through WPA or WPA2, but do not have an existing 802.1X infrastructure, there is an option for you. You can take advantage of one of the Wi-Fi security services designed for this niche. One example is the SecureMyWiFi service from WiTopia, which offers a RADIUS authentication and security key distribution service for a modest annual fee.

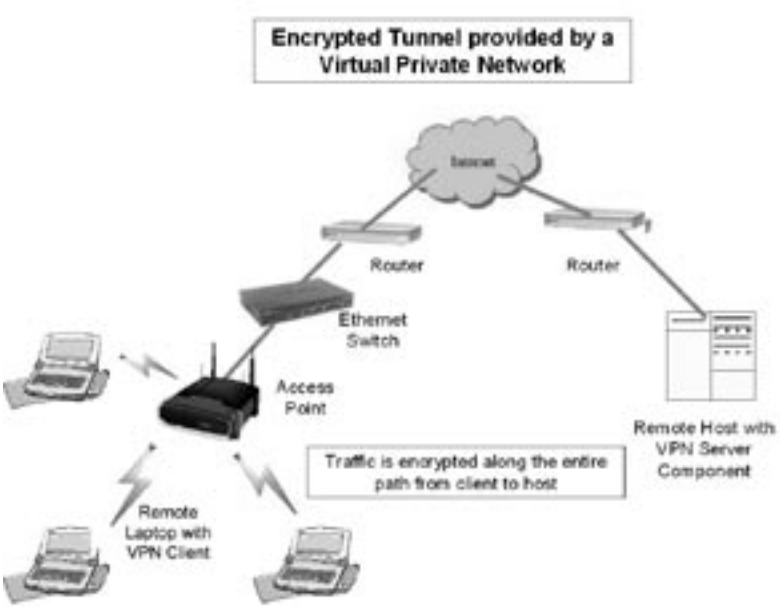

Figure 9
Illustration of the encryption route provided by a Virtual Private Network (VPN). The red bolts and lines indicate the entire line of transmission is encrypted.

Scope of Protection

Keep in mind the above-mentioned security protocols do not provide encryption beyond the wireless network. Consider the case in which you use the wireless network to connect your laptop to your organization's LAN and, in turn, to the Internet. The wireless LAN security measures encrypt the traffic only between the radio on your laptop and the access point. The information is not encrypted on the wired network, on the Internet, or on the remote server's network. Enabling WEP, WPA, or any other security protocol on the wireless network does not provide the end-to-end encryption needed to transmit sensitive information. Figure 8 illustrates the scope of protection provided through WLAN security.

Virtual Private Networks

A security scheme that was around long before wireless LANs, but one especially well suited for them, is the Virtual Private Network, or VPN. A VPN establishes a secure channel of communication that enables information to travel safely through insecure networks. The goal of the VPN is to create a secure end-to-end tunnel between the user's computer and the internal network of the organization. That secure tunnel can traverse less secure networks within the organization, the Internet, or other questionable networks.

A VPN is established through software on both ends of the tunnel; that software encrypts and decrypts the data stream. One side of the VPN will reside within the organization's internal network, typically on a firewall or other security server in the data center. The other end of the VPN will reside on the remote user's computer—with the VPN software installed, configured, and activated. Before it establishes the secure tunnel, the user on the remote end must be authenticated, using a username and password sequence verified through an authentication server or through a digital certificate. The VPN secures only the communications between the user's computer and the specification destination at the other end of the

WEPCrack
http:// wepcrack.sourceforge.net

AirSnort
http://airsnort.shmoo.com

WiTopia
www.witopia.net

VPN. It would not, for example, encrypt communications with other destinations on the Internet. Figure 9 illustrates the tunnel of protection provided through a VPN.

Many remote workers use this approach to gain secure access into their organization's internal systems. Many organizations require the use of a VPN for personnel that telecommute and work at home. VPNs also provide an additional layer of security for mobile workers.

With the assistance of a VPN, one can work with complete security and privacy even across an open wireless LAN. Since the VPN establishes an encrypted end-to-end tunnel, it doesn't matter that the wireless LAN isn't encrypted. The VPN offers better security than even the latest and greatest WLAN security schemes, because its scope is end-to-end.

Within an organization, one might establish a WLAN using WPA2 and 802.1X authentication to provide sufficient security to conduct business operations. This environment would provide a high degree of security since all communications are authenticated and encrypted. But if the organization has an open wireless LAN for public access as part of its network, that network would not be safe for business use. One, however, could safely use that open wireless LAN through a VPN.