The Guts of WLAN Security Policy

You've probably heard the story by now that 802.11 wired equivalent privacy (WEP) is broken and just about anyone can compromise wireless LAN (WLAN) resources. What you've heard is absolutely true, especially if you don't implement techniques that will counter the known weaknesses. With any WLAN, you need to consider policies that will protect resources from unauthorized people. Here's a look at what you should include.

Activate WEP at the very least. WEP has weaknesses, making it inadequate for protecting networks containing information valuable to others. The problem is that 802.11 does not support the dynamic exchange of WEP keys, leaving the same key in use for weeks, months, and years.

There are some good hackers out there who can crack into a WEP-protected network using freely-available tools such as AirSnort and WEPCrack. However, WEP does a good job of protecting many home and business networks from the general public. To crack WEP, you need to know how to use the complicated tools and capture a lot of network packets , something that most people won't bother with unless the network resources are extremely valuable and they have infinite patience. The use of standard 802.11 WEP for networks where there is low risk of attack by actual hackers is a minimum for any security policy.

Utilize dynamic key exchange mechanisms. Until 802.11i is finalized, you need vendor-specific technologies for enhanced encryption and dynamic key exchange. Do this if you're concerned about someone going out of his or her way to access your network. The 802.11i committee is working on a revision to the 802.11 standard that will provide advanced security features, including the use of the Advanced Encryption Standard (AES) and dynamic key exchange. This standard, though, will not likely be in commercial products until late 2003. Even the 802.11i subset called Wi-Fi Protected Access, which should work on many existing WLAN products, won't be available until February 2003 at the earliest. You need to utilize vendor-specific solutions in the meantime.

Ensure NIC and access point firmware is up-to-date. Vendors often implement patches to firmware that fix security issues. Start by upgrading the firmware in the access point soon after pulling it out of the box. On an ongoing basis, make it a habit to check that all devices have the most recent firmware releases to cover up all known security holes. Of course this is why it's a good idea to make certain you can easily upgrade the firmware in the access points that you purchase.

Ensure only authorized people can reset the access points. Some access points will revert back to factory default settings (i.e., no security at all)

when someone pushes the reset button on the access point. This makes the access point a fragile entry point for a hacker to extend their reach into the network. As a result, provide adequate physical security for the access point hardware. For example, don't place an access point within easy reach on a table in the office. Instead, mount them out of view above ceiling tiles. Some access points don't have reset buttons, but they allow you to reset via an RS-232 cable through a console connection. To prevent this, be sure to disable the console port.

Properly install all access points. Don't leave access points within easy reach of a hacker who can replace a legitimate safeguarded access point with an unsecured, rogue access point that accepts access from any user. In fact, it's a good idea to conceal the access point as much as possible to make it more difficult for a hacker to find. Be sure, however, to note the location of the wireless hardware; otherwise, you'll have a difficult time finding them yourself.

Disable access points during non-usage periods. If possible, shut down the access points when users don't need them. This limits the window of opportunity for a hacker to use an access point to their advantage as a weak interface to the rest of the network. You could simply pull the power plug on each access point; however, consider deploying power-over-Ethernet (PoE) equipment that provides this feature via centralized operational support tools.

Assign "strong" passwords to access points. Don't use default passwords for access points. They are also well known, making it easy for someone to change configuration parameters on the access point to their advantage. Be sure to alter these passwords periodically. Ensure passwords are encrypted before being sent over the network.

Don't broadcast SSIDs. If this feature is available, you can avoid having user devices automatically sniff the SSID in use by the access point. WindowsXP and other monitoring tools (e.g., AirMagnet, NetStumbler, and AiroPeek) will automatically sniff the 802.11 beacon frames to obtain the SSID. With SSID broadcasting turned off, the access point will not include the SSID in the beacon frame, making most sniffing tools useless. This isn't foolproof, however, because someone can still monitor 802.11 association frames (which always carry the SSID, even if SSID broadcasting is turned off). At least shutting off the broadcast mechanism will limit access.

Don't use default SSID names. As a default setting, most access point vendors use their vendor name (e.g., "Proxim" or "Symbol") as the SSID. Others are also commonly known -- such as "Any." As a result, set the SSID to something different ---- as odd an word or phrase as possible -- to

avoid people from guessing. Think of the SSID as being a weak password that will stop a casual snooper. A hacker, though, can easily find the SSID in association frames when a user first boots their wireless device.

Reduce propagation of radio waves outside the facility. Through the use of directional antennas, you can direct the propagation of radio waves inside the facility and reduce the "spillage" outside the perimeter. This not only optimizes coverage, it also minimizes the ability for a snooper outside the controlled portion of the company to eavesdrop on user signal transmissions or interface with the corporate network through an access point. This also reduces the ability for someone to jam the WLAN from outside the perimeter of the facility. Consider setting access points near the edge of the building so you can lower transmit power and thus reduce range outside the facility.

Deploy access controllers. Access points that are only compliant with the 802.11 standard offer inadequate authentication. In fact, 802.11 only authenticates a radio NIC to an access point, not the other way around. Thus, consider the use of an access controller from vendors such as ReefEdge, Bluesocket, and Nomadix. These devices offer tough access control to the network while interfacing with authentication servers such as RADIUS. Some vendors also include these types of access control functions within their enterprise grade access points.

Implement personal firewalls. If a hacker is able to associate with an access point, which is extremely probable if WEP is turned off, the hacker can easily access (via the Windows operating system) files on other users' devices that are associated with an access point on the same WLAN. As a result, it's crucial that all users disable file sharing for all folders and utilize personal firewalls.

Utilize IPSec-based Virtual Private Network (VPN) technology on client devices. If needing to access sensitive applications, users should install VPN software to provide proper levels of encryption and access control. This is especially needed for users operating from remote locations, such as public WLANs in airports and convention centers. Most public WLANs are very open and don't provide any encryption mechanisms.

Utilize static IP addresses for clients and access points. A common method for assigning IP addresses is to implement dynamic host configuration protocol (DHCP). DHCP offers a convenient way to distribute IP addresses to client devices. The problem, though, is that this also makes it very easy for a hacker to become connected to the network. Static IP addresses at least makes it more difficult.

Monitor for rogue access points. Utilize operational support tools to continually monitor the network and check for access points that don't conform to configuration policies. An access point that doesn't match specific security settings has likely been reset or is actually a rogue access point installed by a hacker or an employee not wanting to coordinate with IT personnel.

If access points are found with improper settings, restore the settings as soon as possible. Be sure to secure management traffic, however, through the use of Simple Network Management Protocol (SNMP) or similar protocols. You can also deploy intrusion detection sensors, available in some operational support tools, to identify the presence of hackers based on invalid MAC addresses. The main idea is to provide alerts if suspicious behavior is occurring. Monitor from the wireless and wired side of the network. For example, you can use a wireless sniffing tool, such as AirMagnet's WLAN Analyzer or AiroPeek NX, and walk throughout the facility while capturing access point configurations.

An issue here is that some companies have networks that span large geographic areas, such as worldwide. So define a method for scanning for suspicious-looking devices from the wired side of the network.

Control the deployment of WLANs. Ensure that all employees and organizations within the company coordinate the installation of WLANs with the appropriate information systems group. Forbid the use of unauthorized access points. Mandate the use of approved vendor products that you've had a chance to verify appropriate security safeguards. Maintain a list of authorized radio NIC and access point MAC addresses that you can use as the basis for identifying rogue access points.

With these recommendations in mind, you have a basis for forming a solid security policy. When deciding on which techniques to implement, however, consider the actual security needs. For example, WEP may be good enough for home and small business WLANs. If you're a financial institution or retail store transmitting sensitive data, then you'd better concentrate on using a proprietary, dynamic form of WEP, at least for now.