AN AIRMAGNET TECHNICAL WHITE PAPER

The Top Seven Security Problems of 802.11 Wireless

by Matthew Gast

WWW.AIRMAGNET.COM

Table of Contents

The AirMagnet Wireless LAN Analyzer

Seven Security Problems Revisited:
Using a Wireless Analyzer to Address Security Vulnerabilities
in 802.11a and 802.11b Radio Bands

The stunning success of 802.11 is based on its development as "wireless Ethernet," which made it instantly familiar to the large community of Ethernet LAN administrators. As 802.11 continues its ascent, though, its differences from Ethernet are becoming more apparent. Many of these differences are due to the relative unfamiliarity of many network administrators with the radio frequency physical layer. While all network administrators must gain a basic understanding of the radio link, a number of tools are beginning to incorporate critical radio analysis functions to help them in this task. Wireless network analyzers have long been an indispensable tool for network engineers in troubleshooting and protocol analysis. Many analyzers have added some security functionality that allows them to take on security audit functions as well. Products are now filling out the security role and moving into radio management by taking advantage of the fact that they are often used around trouble spots or to diagnose user complaints.

In May of this year, I wrote a short article for the O'Reilly Network titled "Seven Security Problems of 802.11 Wireless."[1] The article discussed seven of the most prominent security vulnerabilities associated with wireless LANs, as well as how network engineers could build a secure wireless network. Many of the questions I receive about that article are about the tools that network administrators can use. As with any other type of network, an analyzer is one of the first purchases that a wireless network administrator should make. In addition to the traditional functions of protocol analysis and diagnostic tool, wireless network analyzers can be used to

[1] A copy of the article is available from http://www.oreillynet.com/pub/a/wireless/2002/05/24/wlan.html

address many of the security concerns that may hinder wireless network deployment. This article reexamines each of the security problems from the original "Seven Security Problems" and describes how and why a wireless analyzer is a vital tool for ensuring the security of wireless networks.

Problem #1: Easy Access

Wireless LANs are easy to find. To enable clients to find them, networks must transmit Beacon frames with network parameters. Of course, the information needed to join a network is also the information needed to launch an attack on a network. Beacon frames are not processed by any privacy functions, which means that your 802.11 network and its parameters are available for anybody with an 802.11 card. Attackers with high-gain antennas can find networks from nearby roads or buildings and may launch attacks without having physical access to your facility.

Solution #1: Enforce Strong Access Control

Easy access does not need to be synonymous with vulnerable. Wireless networks are designed for connectivity, but can be tightened dramatically if your security policy calls for it. At the most extreme, a wireless network could be confined to an electromagnetically shielded room that does not allow perceptible levels of RF leakage. For most institutions, however, such lengths are not necessary. Ensuring that wireless networks are subject to strong access control can mitigate the risk of wireless network deployment. Ensuring security on a wireless network is partly a matter of design. Networks should place access points outside of security perimeter devices such as firewalls, and administrators should consider using VPNs to provide access to the corporate network. Strong user authentication should be deployed, preferably using new products based on the IEEE 802.1x standard. 802.1x defines new frame types for user-based authentication and leverages existing enterprise user databases, such as RADIUS. "Front end" authentication exchanges using 802.1x over the wireless medium are converted to

RADIUS requests over the "back end" wired LAN. Traditional wired analyzers can provide insight into the authentication process by looking at RADIUS requests and responses, but very few products can provide the same level of insight into the front end exchange over the wireless medium. AirMagnet's AirWISE expert analysis system for 802.11 authentication includes a specific diagnostic routine for wireless LANs that watches authentication traffic and provides a diagnostic for network administrators that does not require painstaking analysis of frame decodes. The expert analysis system, which tracks 802.1x authentication messages and key distribution messages from a central screen, has proven to be invaluable for wireless LAN deployments using 802.1x, such as the Interop Labs' wireless LAN security project.[2]

Any design, no matter how strong, must be regularly audited to ensure that the actual deployment is consistent with the security objectives of the design. The AirWISE analysis engine will perform in-depth analysis on frames and can detect several common 802.11 security problems. Although a number of WEP attacks have been well-publicized in the past year, vendor patches are available which address all known weaknesses in WEP. AirMagnet's expert analysis identifies known weak WEP implementations by alerting administrators to implementations that reuse IVs, have a predictable IV pattern, or use "weak" IVs that provide information to WEP cracking programs such as AirSnort. By identifying weak implementations, administrators can apply the appropriate firmware upgrades to maintain network security.

Inappropriate configurations may be a major source of security vulnerability, especially if wireless LANs have been deployed without oversight from security

[2] For more details on the iLabs wireless security project, see http://www.ilabs.interop.net/details?topic=WLAN_Sec

engineers. AirMagnet's expert engine can detect when factory default configurations appear to be in use, which may help auditors track down access points that have not been configured to use any security features. To aid in security audits, AirMagnet 1.5 also records alarms when it spots devices that are not using strong security measures, such as VPNs or 802.1x.

Problem #2: "Rogue" Access Points

Easy access to wireless LANs is coupled with easy deployment. When combined, these two characteristics can cause headaches for network administrators and security officers. Any user can run to a nearby computer store, purchase an access point, and connect it to the corporate network without authorization. Many access points are now priced well within the signing authority of even the most junior managers. Departments may also be able to roll out their own wireless LANs without authorization from a central IT organization. So-called "rogue" access deployed by end users poses great security risks. End users are not security experts, and may not be aware of the risks posed by wireless LANs. Many deployments that have been logged and mapped by "war drivers" do not have any security features enabled, and a significant fraction have no changes from the default configuration.

Solution to #2: Regular Site Audits

Like any other network technology, wireless networks require vigilance on the part of security administrators. Given the ease with which many of these technologies can be exploited for network access, learning when unauthorized networks have been deployed is a task of great importance.

The obvious way to find unauthorized networks is to do the same thing that attackers do: use an antenna and look for them so that you find unauthorized networks before attackers exploit them. Physical site audits should be conducted as frequently as possible. The tradeoff is that more frequent audits are more likely to catch unauthorized deployments, but the high cost of staff time may make walk-through detection untenable in all but the most sensitive environments. One potential compromise is to select a tool based on a small handheld form factor such as the Compaq iPAQ, and have help desk technicians use handheld scanners to detect unauthorized networks while responding to user support calls throughout the campus.

Walkthrough detection often begins with NetStumbler (http://www.netstumbler.com). NetStumbler is an excellent tool for finding large numbers of access points and associating them with geographic locations for mapping applications, but it is a limited tool for the professional network administrator. Current versions of NetStumbler rely on active probing to discover access points, but many access points can be configured to ignore such requests. AirMagnet uses passive analysis to discover AP transmissions in the air, and will uncover any access point within range of its antenna.

One of the biggest changes in the 802.11 market this year was the emergence of 802.11a as a viable commercial product. That success drives a need to provide tools for administrators running 802.11a networks. Fortunately, 802.11a uses the same MAC as its more widely deployed predecessors, so much of what administrators know about 802.11 and their current analyzer solution will transfer over seamlessly. Mature commercial products, including the AirMagnet analyzer, have now released software versions that support 802.11a. Administrators should look for a hassle-free product that supports both 802.11a and 802.11b in the same package, preferably simultaneously. Dual-band 802.11a/b chipsets and cards built with them allow analyzers to work on both bands without hardware changes, which means that network administrators need to buy and learn only one supported platform for both 802.11a and 802.11b. This trend should continue to 802.11g as well, when analyzer vendors are certain to adopt 802.11a/b/g cards.

Many tools can be used to perform site audits and track rogue access points, but network administrators must be conscious of the need to keep up with the latest techniques used in the cat-and-mouse game played out in the site audit. Access points can be deployed in any frequency band defined in 802.11, so it is important that any tools used in audits can scan the entire frequency range. Even if you have chosen to deploy 802.11b, an analyzer used for site audit work should be capable of simultaneously scanning for unauthorized 802.11a access points so that no hardware or software swaps are required during an audit.

Some rogue access points are beginning to be deployed illegally on 802.11b channels that are not available for transmission. For example, the FCC rules only allow the use of 802.11b channels 1 through 11. Channels 12 through 14 are defined in the specification, but are only available for use in Europe and Japan. Some users may, however, deploy an access point on the European or Japanese channels in the hope that a site audit focused on the FCC-allowed channels will overlook higher frequency channels. It is especially important to track any devices that are deployed outside the authorized frequency band to avoid enforcement actions taken by regulatory authorities. Passive analyzers, such as the AirMagnet, are a valuable tool because they will detect illegal deployments, but do not transmit any power and thus are themselves legal to use.

Network administrators are always pressed for time, and need a convenient way to find rogue access points while ignoring authorized access points. AirMagnet's expert engine allows administrators to configure a list of authorized access points. Any unauthorized access point will trigger an alarm. In response to the alarm, network administrators can use the Find tool on an AirMagnet to home in on an access point or station based on real-time signal strength meters. Although the Find tool is not incredibly accurate, it is generally good enough to narrow down the search area to one of a few cubicles.

Problem #3: Unauthorized Use of Service

Several war drivers have published results indicating that a clear majority of access points are put in service with only minimal modifications to their default configuration. Nearly all of the access points running with default configurations have not activated WEP or have a default key used by all the vendor's products out of the box. Without WEP, network access is usually there for the taking. Two problems can result from such open access. In addition to bandwidth charges for unauthorized use, legal problems may result. Unauthorized users may not necessarily obey your service provider's terms of service, and it may only take one spammer to cause your ISP to revoke your connectivity.

Solution to #3: Design and Audit for Strong Authentication

The obvious defense against unauthorized use is to prevent unauthorized users from accessing the network. Strong, cryptographically protected authentication is a precondition for authorization because access privileges are based on user identity. VPN solutions deployed to protect traffic in transit across the radio link provide strong authentication. Organizations which perform risk assessments that indicate that 802.1x is a sufficient technical countermeasure should nevertheless ensure that a cryptographically secure authentication method is chosen, such as Transport Layer Security (TLS), Protected EAP (PEAP), or Tunneled TLS (TTLS). As part of its monitoring of 802.1x, AirMagnet can detect important 802.1x properties such as the user name and EAP type.

Once a network has been successfully deployed, it is vital to ensure that authentication and authorization policies are rigorously followed. As with the rogue access point problem, the solution is to perform regular audits of the deployed wireless network equipment to ensure that strong authentication mechanisms are in use and that network devices are properly configured. Site audits are a vital component of wireless LAN security because they can be used to verify that strong security tools are in place and are required for use to the wireless

LAN, as well as sniffing out unauthorized wireless LAN deployments. Any comprehensive audit tool must detect access points in both the 802.11b (2.4 GHz ISM band) and 802.11a (5 GHz U-NII) frequency bands as well as summarize operational parameters relevant to security. If an unauthorized station is found connected to the network, a handheld receiver can be used to track down its physical location. Analyzers like the AirMagnet can also be used verify configuration of many access point parameters and raise alarms when access points expose security vulnerabilities.

Problem #4: Service and Performance Constraints

Wireless LANs have limited transmission capacity. Networks based on 802.11b have a bit rate of 11 Mbps, and networks based on the newer 802.11a technology have bit rates up to 54 Mbps. Due to MAC-layer overhead, the actual effective throughput tops out at roughly half of the nominal bit rate. Current shipping access points share that limited capacity between all the users associated with an access point. It is not hard to imagine how local-area applications might overwhelm such limited capacity, or how an attacker might launch a denial of service attack on the limited resources.

Radio capacity can be overwhelmed in several ways. It can be swamped by traffic coming in from the wired network at a rate greater than the radio channel can handle. If an attacker were to launch a ping flood from a Fast Ethernet segment, it could easily overwhelm the capacity of an access point. By using broadcast addresses, it is possible to overwhelm several directly connected access points. Attackers could also inject traffic into the radio network without being attached to a wireless access point. The 802.11 MAC is designed to allow multiple networks to share the same space and radio channel. Attackers wishing to take out the wireless network could send their own traffic on the same radio channel, and the target network would accommodate the new traffic as best it could using the CSMA/CA mechanisms in the standard. Malicious attackers who transmit spoofed frames can also overwhelm limited capacity. Attackers may also opt for simple radio jamming techniques and send high noise transmissions at a target wireless network.

Large traffic loads need not be maliciously generated, either, as any network engineer can tell you. Large file transfers or complex client/server systems may transfer large amounts of data over the network to assist users with their jobs. If enough users start pulling vast tracts of data through the same access point, network access begins to resemble the caricature of dial-up access used by purveyors of high-speed broadband services.

Solution to #4: Monitor the Network

Addressing performance problems starts with monitoring and discovering them. Administrators have many channels for performance data ranging from purely technical measures such as SNMP to non-technical but potentially potent measures such as user performance reports. One of the major problems with many technical measures is the lack of detail required to make sense of many end user performance complaints. Wireless network analyzers can be a valuable ally for the network administrator by reporting on the signal quality and network health at the current location. AirMagnet's analyzer can break the received traffic down by either transmission speed or frame type. Large amounts of low-speed transmissions may indicate external interference, severe multipath fading, or that the station is simply too far away from the access point. The ability to display instantaneous speeds on each channel gives a strong visual depiction of the remaining capacity on the channel, which easily shows whether a channel is crowded. Excessive traffic on an access point can be addressed by segmenting the access point's coverage area into smaller coverage areas, or by applying a traffic shaping solution at the confluence of the wireless network with the corporate backbone.

While no technical solution exists to the vulnerabilities resulting from the lack of authentication of control and management frames, administrators can take steps to deal with them. Analyzers are often used near trouble spots to aid in diagnosis, and are ideally positioned to observe many denial of service attacks. Several management and control frames are not authenticated, and there is no mechanism in 802.11 to ensure that traffic with a particular source address has not been forged. Attackers can exploit this by crafting custom 802.11 frames using one of several commonly available 802.11 programming interfaces. One security researcher has even written a tool that spoofs the disassociation messages transmitted by access points to clients. Without cryptographic authentication of disassociation messages, clients will respond to these forged messages by disconnecting from the network. Until cryptographic frame authentication of every transmitted frame is required by the standards, the only practical defense against flooding attacks is to locate attackers and apply an appropriate solution. AirMagnet 2.5 has several built-in alarms for detecting malicious floods of unauthenticated control and management frames, as well as high levels of noise. Its expert analysis engine can also identify malicious clients attempting to launch denial of service attacks against access points.

Problem #5: MAC Spoofing and Session Hijacking

802.11 networks do not authenticate frames. Every frame has a source address, but there is no guarantee that the station sending the frame actually put the frame "in the air." Just as on traditional Ethernet networks, there is no protection against forgery of frame source addresses. Attackers can use spoofed frames to redirect traffic and corrupt ARP tables. At a much simpler level, attackers can observe the MAC addresses of stations in use on the network and adopt those addresses for malicious transmissions. To prevent this class of attacks, user authentication mechanisms are being developed for 802.11 networks. By requiring authenticating by potential users, unauthorized users can be kept from accessing the network. The basis for user authentication is the 802.1x standard ratified in June 2001. 802.1x can be used to require that users authenticate before accessing the network, but additional features are necessary to provide all of the key management functionality required by wireless networks. The additional features are currently being ironed out by Task Group I for eventual ratification as 802.11i.

Attackers can use spoofed frames in active attacks as well. In addition to hijacking sessions, attackers can exploit the lack of authentication of access points. Access points are identified by their broadcasts of Beacon frames. Any station which claims to be an access point and broadcasts the right service set identifier (SSID, also commonly called a network name) will appear to be part of an authorized network. Attackers can, however, easily pretend to be an access point because nothing in 802.11 requires an access point to prove it really is an access point. At that point, the attacker could potentially steal credentials and use them to gain access to the network through a man-in-the-middle (MITM) attack. Fortunately, protocols that support mutual authentication are possible with 802.1x. Using methods based on Transport Layer Security (TLS), access points will need to prove their identity before clients provide authentication credentials, and credentials are protected by strong cryptography for transmission over the air. Session hijacking will not be completely solved until the 802.11 MAC adopts per-frame authentication as part of 802.11i.

Solution to #5: Adopt Strong Protocols and Use Them

Until the ratification of 802.11i, MAC spoofing will be a threat. Network engineers must focus on containing any damage done by MAC spoofing by isolating wireless networks from the more vulnerable core network. AirMagnet can detect AP spoofing and is configured by default to raise an alarm to alert administrators to investigate further. In the same time frame, session hijacking can be prevented only by using a strong cryptographic protocol such as IPSec. As part of its analysis of captured frames, the AirMagnet analyzer can determine what security level is in use, which enables network administrators to tell at a glance if the desired security protocols are in use.

In addition to using strong VPN protocols, you may wish to require the use of strong user authentication with 802.1x. During the pilot project phase, AirMagnet's detailed analysis of the 802.1x authentication status provides a valuable check on the wireless component of the 8021x authentication exchange. When performing site audits after deployment, the AirMagnet analyzer will decode the authentication type, which allows network administrators to ensure that passwords are protected by strong cryptography.

Problem #6: Traffic Analysis and Eavesdropping

802.11 provides no protection against attacks which passively observe traffic. The main risk is that 802.11 does not provide a way to secure data in transit against eavesdropping. Frame headers are always "in the clear" and are visible to anybody with a wireless network analyzer. Security against eavesdropping was supposed to be provided by the much-maligned Wired Equivalent Privacy (WEP) specification. A great deal has been written about the flaws in WEP. It protects only the initial association with the network and user data frames. Management and control frames are not encrypted or authenticated by WEP, leaving an attacker wide latitude to disrupt transmissions with spoofed frames. Early WEP implementations are vulnerable to cracking by tools such as AirSnort and WEPcrack, but the latest firmware releases from most vendors eliminate all known attacks. As an extra precaution, the latest products go one step farther and use key management protocols to change the WEP key every fifteen minutes. Even the busiest wireless LAN does not generate enough data for known attacks to recover the key in fifteen minutes.

Solution to #6: Perform Risk Analysis

When addressing the threat of eavesdropping, the key decision is to balance the threat of using only WEP against the complexity of deploying a more proven solution. Although the current firmware releases address all known vulnerabilities, the same statement could have been made before the drastic break in August 2001. The current state of the art in link layer security is WEP with long keys and dynamic re-keying. WEP has been extensively studied and the security protocols have been fortified against all known attacks. A critical component of this fortification is the short re-keying time, which prevents attackers from learning a great deal about the properties of a WEP key before it is replaced.

If you elect to use WEP, you should audit your wireless network to ensure that it is not susceptible to the AirSnort attack. AirMagnet's analysis engine automatically analyzes all received traffic and checks for known weaknesses in WEP-protected frames. On an ongoing basis, the AirMagnet analyzer will also flag access points and stations with WEP disabled so that they can be investigated further by network administrators. Short re-key times are a crucial tool used in reducing the risks associated with wireless LANs. As part of a site audit, network administrators can use AirMagnet to ensure that any policies on WEP re-keying are implemented by the equipment.

If your wireless LAN is being used for sensitive data, WEP may very well be insufficient for your needs. Strong cryptographic solutions like SSH, SSL, and IPSec were designed to transmit data securely over public channels and have proven resistant to attack over many years, and will almost certainly provide a higher level of security. AirMagnet's access point display can distinguish between access points that use WEP, 802.1x, and VPN technology, which enables network administrators to check that policies that mandate strong cryptography are being followed.

Problem #7: Higher Level Attacks

Once an attacker gains access to a wireless network, it can serve as a launch point for attacks on other systems. Many networks have a hard outer shell composed of perimeter security devices that are carefully configured and meticulously monitored. Inside the shell, though, is a soft, vulnerable center. Wireless LANs can be deployed quickly if they are directly connected to the vulnerable backbone, but that exposes the network to attack. Depending on the perimeter security in place, it may also expose other networks to attack, and you can bet that you will be quite unpopular if your network is used as a launch pad for attacks on the rest of the world.

Solution to #7: Protect the Core from the Wireless LAN

Due to the susceptibility of wireless LANs to attack, they should be treated as untrusted networks. Many companies provide guest access ports in training rooms or lobbies. Wireless LANs can be treated as conceptually similar to guest access ports due to higher probability of access by untrustworthy users. Place the wireless LAN outside the corporate security perimeter and use strong, proven access control technology such as a firewall between the wireless LAN and the core network, and then provide access to the core network through proven VPN solutions.

Conclusion

A common theme throughout this discussion of security problems is that the technological mechanisms to address many of the perceived flaws exist and are well understood, but they must be activated to provide protection. Reasonable precautions can make wireless networks safe for any organization that wants to reap the benefits of mobility and flexibility. As with many other network technologies, the key is to design the network with security in mind and perform regular audits to ensure that the design is the actual basis for deployment. From analysis to troubleshooting to auditing, a wireless network analyzer is an indispensable tool for a wireless network engineer.

About AirMagnet, Inc.

Founded in 2001, AirMagnet, Inc. provides the most trusted WLAN management and security software systems for the enterprise in handheld, laptop and distributed configurations. Used by IT professionals at more than 2,600 companies worldwide in manufacturing, financial, retail, service, health care, utility, transportation, education and government sectors, AirMagnet solves Wi-Fi connection problems, tracks down unauthorized access, simplifies site surveys, and locks in unprecedented levels of network performance, security and reliability. Additional information about AirMagnet and its products is available on the Web at www.AirMagnet.com.