



AN AIRMAGNET TECHNICAL WHITE PAPER

WHAT HACKERS DON'T WANT YOU TO KNOW ABOUT SECURING YOUR WIRELESS LAN



supplied and supported by

Phoenix Datacom

www.phoenixdatacom.com

01296 397711

info@phoenixdatacom.com

www.AirMagnet.com

Despite, media hype, it is possible to secure your enterprise wireless network but it is important to understand that this is a process and not a simple step that you take once. You must be able to actively evaluate your WLAN's potential weak spots at any given moment and minimize threats by deploying an effective intrusion prevention system. This includes intelligent and active defenses that work to maintain and truly secure your enterprise wireless network. That being said, there is no silver bullet that will provide an 100% guarantee but there are smarter ways to approach security.

Securing your wireless network requires a multi-tiered approach that includes:

- Encryption
- Intrusion prevention technology
- User education
- Securing all laptops and mobile devices
- Staying abreast of advances in technology that provide hackers with new opportunities

Is the Hacker Threat Real?

Outside of the IT department, corporate employees seem to think that “hacker” is just the 21st Century word for “the Boogeyman.” Unfortunately, the threat is very real. Hackers have created a strong shadow-community that is so well organized they have their own conventions. DefCon, the largest of these, attracted thousands of hackers (and assorted types who like to keep an eye on hackers) this past August (2004) in Las Vegas. The official DefCon position is that the organizers do not condone criminal activity of any kind. A brief tour around some of the hacker sites (see sidebar, “Windows Into the World of Hackers”) reveals that plenty of such discussions take place all the time in a large and very active community.

What do hackers want? As a group, they want freedom from the niggling little rules the rest of the world plays by. They often use the pirate's skull-and-crossbones as a symbol of their swashbuckling quest for booty. (DefCon's logo is a smiley-face-and-crossbones.) Booty, in the case of hackers, ranges from stealing free bandwidth from your WLAN, to theft of financial and other confidential information, to wholesale piracy of your network. At their most benign, hackers just want to prove they can penetrate your defenses. At their most malevolent, they can wreak millions of dollars worth of damage. Who wants to take the chance that the next war driver probing for an Access Point (AP) signal is just a harmless guy who gets his kicks out of filching a bit of your bandwidth?

Wireless connectivity opened up a whole new wonderful world to hackers. A wired network can only be hacked through a physical connection, usually through the Internet. It requires a fairly high level of skill to break through a company's security gateway and firewall (unless the hacker has obtained a password and MAC¹ address from an unwitting user – more on this later). A toolbox full of hacker freeware like "Net-Stumbler" quickly became available, enabling hackers to break encryption, detect wireless WLAN signals, and gain access to passwords, MAC addresses and SSIDs (Service Set Identifiers) — and full access to corporate data. War drivers, cruising around with laptops and antennae, "sniff" out wireless networks and connect to them. War chalkers, like the hobos of the 1930's who chalked symbols on the houses where they could obtain a free lunch, chalk on the walls of buildings to indicate the presence of unsecured WLANs.

Perhaps the majority of these rogue users are merely stealing bandwidth. For obvious reasons, corporate losses due to wireless network hacking are underreported. A recent survey by KPMG found that 12% of hackers attempted malicious activities², e.g. Denial of Service (DoS) attacks, destruction of data, espionage, theft of financial information or identity theft. The seventh annual Computer Crime and Security Survey undertaken by the FBI and the Computer Security Institute of San Francisco (CSI) found that out of 503 U.S. computer security professionals polled, 90% reported network security breaches within the last 12 months of the survey, while 80% admitted to financial losses due to security breaches. The 44% of respondents who quantified financial losses reported a total of \$445,848,000 lost.³

Happily, the eighth annual survey by CSI and the FBI shows that financial damages from attacks on networks have dropped for the fourth straight year in a row. The survey reported that one of the reasons was an increasing percentage of respondents (73%) have implemented intrusion detection/prevention technology. The previous year, only 60% reported implementing intrusion detection/prevention technology.⁴

How Hackers Attack the Wireless Network

Being an innovative group, hackers are continually coming up with new ways to penetrate network defenses. But their attacks can generally be grouped into these categories:

- MAC spoofing
- Denial of Service
- Malicious association
- Man-in-the-middle attacks

¹ The MAC (Media Access Control) address is a unique identifier for a network device.

² *Computer Weekly*, Feb. 10 2004 p30

³ *National Underwriter Life & Health-Financial Services Edition*, June 17, 2002, v106 i24 p30.

⁴ *Government Computer News*, Sept. 29, 2003, v22 i29 p32.

MAC Spoofing: Hackers use MAC spoofing to impersonate a legitimate network user. All network interface cards (NICs), like PCMCIA or PCI cards, provide a mechanism for changing their MAC addresses, issued by the manufacturer, that identify a specific device. In many cases, the MAC address is used as an authentication factor in granting the device access to the network, or to a level of system privilege to a user.

The hacker will change his device's MAC address to that of a user and thus gain access to the network. If the hacker is using the MAC address of a top executive with access privileges to sensitive material, a great deal of damage can be done.

Attackers employ several different methods to obtain authorized MAC addresses from the network. A brute force attack uses software that will try a string of random numbers until one is recognized by the network. Another way is to monitor network traffic and fish out the authorized MAC addresses.

Denial of Service Attacks: DoS attacks may be launched merely as a form of vandalism, to prevent legitimate users from accessing the network, or they may be carried out to provide cover for another type of attack. In Layer 1 DoS attacks, the hacker uses a radio transmitter to jam the network by emitting a frequency in the 2.4GHz or 5GHz spectrum. As 802.11 equipment operates at a certain signal-to-noise ratio, when the ratio drops below that threshold, the equipment will not be able to communicate.

In a more common type of DoS attack, the hacker uses a laptop or PDA with a wireless NIC to issue floods of associate frames to take up all available client slots in the AP, severing the AP's association with legitimate users. Alternatively, the hacker issues floods of de-association frames, forcing clients to drop their association with the AP. Either way, if the attack is successful, the hacker now controls access to the network.

Malicious Association: The hacker configures his device to behave as a functioning AP. When a user's laptop or station broadcasts a probe for an AP, it encounters the hacker's device, which responds with an association. At this point, the legitimate user's computer can be mined for any and all information, including MAC address, SSID, pass codes, etc.

Man-in-the-Middle Attacks: The hacker sends a de-authorization to a network device, which drops its association to its AP and begins searching for a new AP. It finds the hacker's station (configured to look like an AP), and associates with it. Using the information garnered from the legitimate device, the hacker's device now associates with the legitimate network AP and the network passes through the rogue user's device, allowing him to change or steal data at will.

Internal Vulnerabilities

It has been estimated that internal users create up to a third of the vulnerabilities of the enterprise WLAN. There is the occasional bad apple that steals information or money from his or her employer, but the majority of internal users are not trying to harm the company; they are just ignorant of the consequences of their actions or failure to take precautions.

For instance, there's Mr. Cowboy, the guy who takes pride in never following the rules and going his own way. This is the person who goes out and buys a cheap AP and sets it up so he can always run at peak performance and doesn't have to share bandwidth with others in his area. The problem with these rogue APs is that they are usually unsecured. They are shipped from the factory with default security settings or with the settings turned off, and Mr. Cowboy didn't reconfigure his AP when he plugged it in. This rogue AP creates a wide-open backdoor into your WLAN. Hackers have no difficulty at all dealing with default security settings, and they waltz right in.

Another potential weakness is the neighboring WLAN that may have one or more APs that associate with your network. Anyone on that neighboring network can peek into your WLAN at will. This includes any hacker that cracks the neighbor's WLAN. Even if you've taken all precautions, your neighbor's WLAN may not be secured.

Employees may telecommute from home using wireless technology, or they may take a laptop to a public "hotspot" like an Internet café to check email or catch up on work. Employees need the right MAC address and password to access the enterprise WLAN. However, if the employee's home computer or laptop is using the factory-set default security or no security, that device becomes a "soft AP," broadcasting the MAC address and password freely to any war driver in the street, or the sniffer sipping a latte at the next table.

The SSID is the unique name of a WLAN. War drivers scan for SSIDs in an attempt to configure their device to look like a legitimate user of that network. If the network administrator has been careless about encryption, the rogue user can access the network. In newer wireless networks, some administrators disable the automatic SSID to prevent hackers from obtaining it. (Though this is a deterrent only to inexperienced or casual hackers.)

APs are shipped from the factory with default security settings, or security settings switched off. Every AP on the network must be individually configured to assure that the network is secure.

In an effort to combat rogue users, some network administrators have set up Virtual Private Networks (VPNs). Using advanced encryption techniques and the public telephone infrastructure, VPNs create an invisible data tunnel from one WLAN locale to another (say, between an enterprise's WLAN in New York and its London site), or between one Intranet and another. VPNs are highly secure. However, if one of the WLANs that it connects is unsecured, the entire system is vulnerable to any hacker that associates with the unsecured network.

Legal Implications

Damage to your enterprise data, theft and espionage are just the beginning of your potential problems once hackers get into your WLAN. Government-mandated legislation provides severe penalties for breach of privacy of confidential records, or loss of mandated documentation.

The Gramm-Leach-Bliley Act (GLBA) was enacted to assure that financial institutions protect the privacy of their customers' financial records. The act requires that such institutions take all reasonable measures to detect, prevent and respond to attacks, intrusions or other systems failures. Failure to do so can result in fines of up to \$11,000 per day or \$10,000 per violation.⁵

The Health Insurance Portability and Accountability Act (HIPAA) affects virtually all health care entities in the United States. It is (in part) intended to protect the privacy of individuals' health records. Any electronic transaction that contains confidential health information of an individual is covered by HIPAA. The act requires clear control of access, policies, procedures and technology to restrict who has access to the information, and requires establishment of security mechanisms to protect data that is electronically transmitted. Violations of HIPAA could cost you \$25,000 per incident.⁶

The Sarbanes-Oxley Act (fondly known as SOX), affects every publicly held company in the U.S. Section 404 of SOX requires businesses to document their financial reporting controls and procedures such that it is comprehensively archived and readily retrievable. Any document — even email — that relates to the auditing process must be archived, along with any data relating to “material events.” If this material is lost or damaged, SOX makes the CEO and CFO personally responsible. Corporate officers potentially face stiff fines and jail sentences for lack of compliance.⁷

Finally, there are liability issues. If a hacker uses your WLAN to launch a Denial of Service attack on another company's network, or to distribute child pornography, your company can be held liable for the crime.

⁵ For more information on the Gramm-Leach Bliley Act, see <http://www.ftc.gov/privacy/glbact/>

⁶ For more information on HIPAA, see <http://www.hipaa.org/>

⁷ For more information about the Sarbanes-Oxley Act, see <http://www.sarbanes-oxley.com>

Encryption

You can't prevent hackers from detecting your WLAN's RF signal. The use of directional antennas can help to control the shape of the signal, but they don't completely solve the problem. You can't prevent detection of your signal, but you can do something to make the contents unreadable by unauthorized "listeners." This makes encryption the first, barebones line of defense. It comes built into your WLAN software. When network traffic is encrypted, it may deter the casual or less-adept intruder who is just looking for an easy target. But relying on encryption alone is risky. The initial standard encryption for wireless networking, Wired Equivalent Privacy (WEP) was hacked within weeks of its release.⁸

The next attempt at standard encryption, IEEE's Wi-Fi Protected Access (WPA) bridged the gap until IEEE's recent ratification of an improved 802.11i standard, WPA2. WPA2 employs a different encryption standard, Advanced Encryption Standard (AES), which reportedly meets Federal Information Processing Standard 140-S specifications for wireless security. However, enterprises with existing LANs may have to purchase new hardware to support AES.⁹

IPSec (Internet Protocol Security) and SSL (Secured Socket Layer) are both encryptions used to create VPNs. VPNs are often used to send corporate data over the Internet in a secure "tunnel" that cannot be read or reproduced by unauthorized users. Web-based SSL uses the public-and-private key encryption system from RSA, which also includes the use of a digital certificate. As any Web-enabled machine can be used to access a SSL based VPN, two-way authentication is not available. Anyone with the correct username and password can access the SSL VPN from any PC connected to the Internet. IPSec works at Layer 3 and secures everything in the network. Unlike SSL, which is typically built into the Web browser, IPSec requires a client installation. IPSec facilitates two-way authentication using DES, a powerful block cipher that is highly resistant to attack because it requires an impractical expenditure of time and resources.

Of course, if the VPN is unsecured at either the network where it begins or the network where it ends, a hacker can waltz right through.

It is the nature of hackers to work long and hard to break encryptions, so it is only a matter of time before someone successfully hacks AES and its successors. Encryption, while necessary, should be viewed as only beginning the task of securing the WLAN.

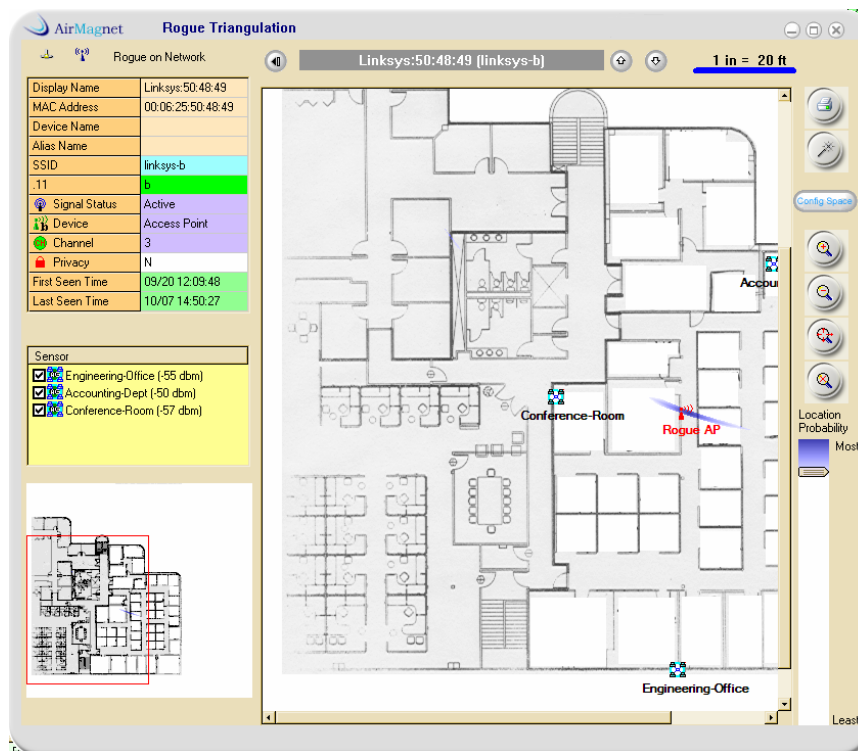
⁸ *RCR Wireless News*, August 2, 2004, v23 i31 p8

⁹ *Ibid.*

Intrusion Prevention

An effective intrusion prevention system monitors your WLAN to allow you to see what's happening in your airspace at all times, assures you that security policies are being followed, sounds the alarm when an intrusion or policy violation is detected, and isolates and cuts off any unauthorized device or user. Wireless LAN infrastructure devices come with some built-in monitoring capabilities, but a specialized overlay monitoring product will provide a richer set of capabilities.¹⁰

Being able to detect rogue and/or neighboring APs associated with your WLAN is essential. Once detected, it is critical to be able to physically locate these APs and take them out (or go have a polite discussion with the administrator of the neighboring WLAN). Locating a rogue AP requires triangulation, made possible by physically locating intelligent sensors around the area covered by the WLAN. Intelligent sensors detect the rogue AP or user, sound the alarm to the network administrator, and isolate the AP until it can be physically removed.



Caption: Triangulating Rogue APs. A screenshot from AirMagnet Enterprise™ shows how AirMagnet's intelligent wireless sensors distributed around the WLAN triangulate and pinpoint the location of a rogue AP. Once the rogue's physical location is known, it can be removed without delay.

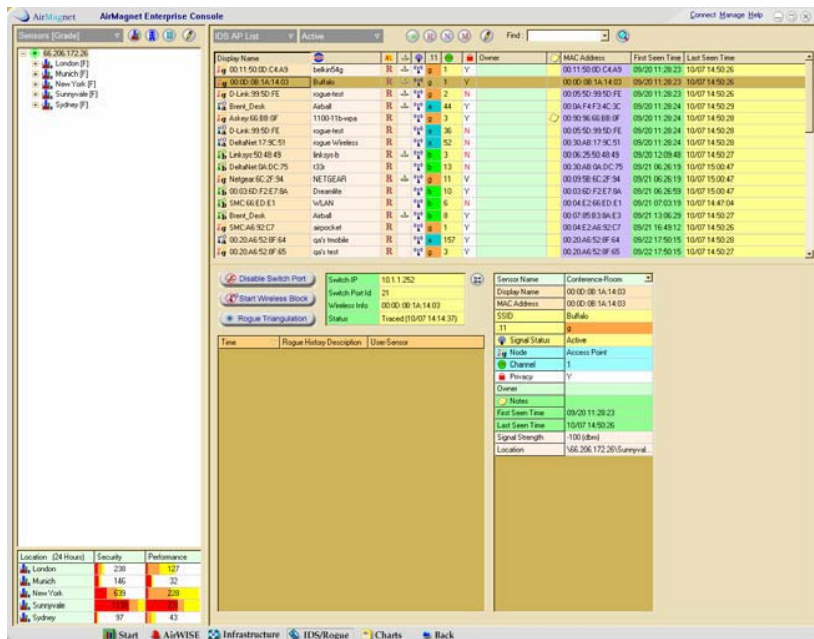
¹⁰ "Watching the Waves," *Network Computing*, Mar. 4, 2004

Intelligent remote sensors can also monitor users/devices and determine whether a user is inside or outside your network perimeter. If a user is outside the perimeter — whether the rogue user is a hacker or a neighbor who has unwittingly associated with your WLAN — the sensor will generate an alarm and isolate the rogue from the network.

One of the most useful aspects of a robust intrusion prevention system is the ability to set security protocols, and modulate the system's response to protocol violation. For instance, the system response to a low-level violation such as multipath detection, which could be merely a malfunctioning AP, might be just an email notification to the administrator, or a log notation. But a high level violation such as a user detected outside the network perimeter might result in a phone call alert.

It's essential to be able to manage WLAN security from a centralized console, where all information is quickly available to the administrator. The system should provide detailed information, such as activity at any single sensor, specifics on any alarm, and a view of network traffic at any given time. Troubleshooting tools, detailed logs, and the ability to measure network performance against established standards are all necessary to good network security. It is especially important to get reports in highly granular detail, customized to the needs of the network administrator. These reports are key to studying network performance and usage over time, pinpointing and eliminating potential trouble spots *before* they become problems.

And the network administrator needs flexibility from an intrusion prevention system. For instance, access privileges granted to a C-level executive need to travel with that executive when he or she works from home or leaves on a business trip. The administrator must be able to configure related alarms into a coordinated policy instead of being limited to a fixed hierarchy. When the network is expanded, the intrusion prevention system must be scaleable to grow with it.



Caption: The Three D's of Intrusion Prevention. Any wireless network, no matter how well protected, can be threatened by rogue devices. The key to preventing intrusion by rogues is the ability to Detect, Disable, and Document every rogue *before* it can cause any damage. AirMagnet Enterprise provides a complete approach to rogue management including: multiple detection mechanisms that immediately expose every rogue; an active blocking suite that disables the rogue both on the wireless and wired side; and a dedicated rogue page that provides consolidated details on every device, including its physical location on a map, wired trace analysis, event history and more.

User Education

There is no technology so sophisticated that human beings can't mess it up. This is particularly true of WLAN security, because users outside the IT department often don't realize that their actions may endanger the company. A sales manager may know a great deal about negotiating deals, but may be unaware that his or her laptop is not securely configured, even though the manager has used the proper passwords and procedures to gain remote access to the WLAN.

So WLAN user education is an important leg on the security stool. Users need to know about security protocols and how to follow them. More critically, users need to know *why* these protocols exist. Going back to Mr. Cowboy, some people believe that rules are made to be broken. Understanding that the use of a rogue AP may enable a hacker to access sensitive corporate data (or steal Mr. Cowboy's bank account number and identity), goes a long way toward gaining user compliance.

Though WLAN security protocol may be set by IT, education and enforcement is best implemented by Human Resources.¹¹ HR is equipped to conduct training on the subject – and to enforce the consequences for infringement. Every enterprise with WLAN technology must develop a serious user training program to assure that users understand that they each have a personal responsibility to keep the enterprise safe from intrusion. Part of that educational process is setting protocol for securing laptops and other wireless devices and banning unauthorized APs.

Keeping up with the Hackers

Hackers may be at best mischievous individualists, and at worst criminals, but they are one of the brightest and most creative groups of humans on the planet. As developers of legitimate technologies work hard to stay ahead of the hackers, the hackers are working harder to figure out how to break the new code.

If you are responsible for WLAN security in your enterprise, it behooves you to spend some time studying the enemy. The easiest way to do this is making routine visits to hacker web sites and to listen in on the chat. You might even attend DefCon or one of the other hacker confabs to get a lead on what hackers are doing. The sidebar on “Windows Into the World of Hackers” lists some places to start.

Above all, the WLAN should be monitored 24x7. You must be able to view any AP’s activities in detail, monitor individual devices associated with your network, and analyze network productivity. You should be able to get detailed information on any anomaly. A great deal rides on your ability to see problems and cut them off before damage can be done.

AirMagnet Enterprise: A Complete Security System for the Enterprise WLAN

AirMagnet Enterprise tames this complexity and exposure with a true zero-tolerance approach to wireless security that is tied to the policies and needs of your business. AirMagnet Enterprise detects every threat in the network, worldwide, and then automatically takes action with multiple layers of automated threat response. An intuitive global interface provides full disclosure of all wireless events, making it easy to make the right decisions while cutting through the time required to manage your networks. The end result is a system that brings simplicity, accountability, and bullet-proof defenses to any wireless investment.

¹¹ “Companies Clamping Down on Wireless Workers who Bypass Encryption,” *Workforce Management*, Dec. 2003, p69.

Detection

AirMagnet Enterprise automatically detects and alarms dozens of types of wireless intrusions, including rogue APs, DoS attacks, spoofed MAC addresses, the use of freeware probing tools and much more.

Prevention

AirMagnet Enterprise gives an alarm appropriate to the detected problem, but automatically moves to isolate and cut off rogue APs and rogue devices before the network is successfully penetrated. Multiple detection mechanisms identify rogues on the basis of MAC address, vendor type, wireless band or SSID. When the system operator arrives on the scene, AirMagnet Enterprise provides tools to physically locate suspect devices so they can be physically removed.

Vulnerability Assessment

WLANs are never static. Because they change from day to day, AirMagnet Enterprise performs a continuous vulnerability assessment of the network, detecting a host of subtle weaknesses that could result in network penetration. The system alerts IT immediately when vulnerability is detected.

Control Over Security Policy

Even one AP or station that does not adhere to security policies puts the entire WLAN at risk. AirMagnet allows you to deploy different security strategies for different individuals or different locations, and monitor for 100% compliance. AirMagnet Enterprise offers 120+ security and performance alerts organized into a logical hierarchy, allowing managers to create and manage a coordinated policy. Each policy level and alarm comes with expert explanation and advice. Alarm notifications can be set to escalate in urgency if a problem gets worse.

About AirMagnet

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

© 2004 AirMagnet, Inc. All rights reserved. AirMagnet and AirWISE are registered trademarks, and the AirMagnet logo is a trademark, of AirMagnet, Inc. All other product names mentioned herein may be trademarks of their respective companies.