

Wireless LAN Security – What Hackers Know That You Don’t

As the next generation of IT networking, 802.11 wireless LANs are also the new playgrounds for hackers. Effective encryption and authentication security measures for wireless LANs are still developing, but hackers already possess easy-to-use tools that can launch increasingly sophisticated attacks that put your information assets at risk.

Like personal computers in the 1980s and the Internet in the 1990s, wireless LANs are the new frontier of technology in the enterprise. Thus, this white paper is not designed to scare enterprises away from deploying wireless LANs. Wireless LANs can be secured with a layered approach to security that goes beyond new encryption and authentication standards to include 24x7 monitoring and intrusion protection.

This white paper outlines how hackers are exploiting vulnerabilities in 802.11 wireless LANs and the widely available hacking tools. The information presented is a collection of already published risks to wireless LANs. This white paper is written to inform IT security managers of what they are up against. In order to effectively secure their wireless LANs, enterprises must first know the potential dangers.

Wireless LANs are a breeding ground for new attacks because the technology is young and organic growth creates the potential for a huge payoff for hackers.

– Pete Lindstrom, Spire Security, Sept. 2002

What’s at Risk?

Wireless LANs face all of the security challenges of any wired networks in addition to the new risks introduced by the wireless medium that connects stations and access points. This white paper focuses on the wireless-specific attacks, threats, and risks.

Any wireless access point attached to a wired network essentially broadcasts an Ethernet connection and an onramp to the entire enterprise network. Layer 1 and Layer 2 of a network is typically protected by the CAT5 wire within a building in a traditional wired network but is exposed in a wireless LAN.

The satellite photograph on this page graphically displays how a radio signals from a single access point can travel several city blocks outside of the building. Without proper security measures for authentication and

encryption, any laptop with a wireless card can connect with the network or stealthily eavesdrop on all network traffic across that access point from any area within the colored areas on the map.

Some enterprises make the mistake of believing that they do not have to worry about wireless security if they are running non-mission critical systems with non-sensitive information across their wireless LANs. However, few networks operate as islands of automation. Most connect with the enterprise backbone at some point, and hackers can use the wireless LAN as a launch pad to the entire network. Thus, every entry point to that network should be secured.

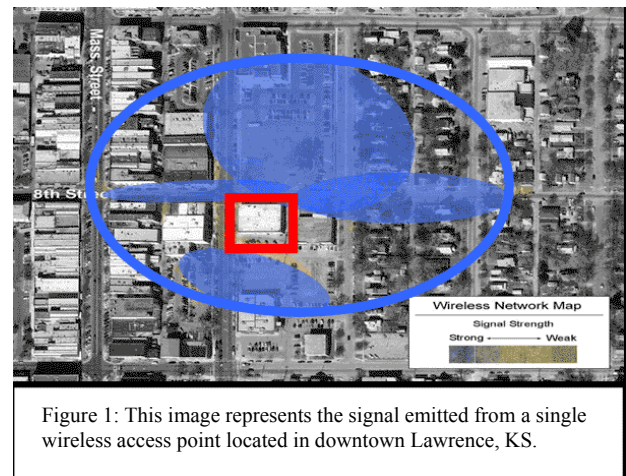


Figure 1: This image represents the signal emitted from a single wireless access point located in downtown Lawrence, KS.

In the summer of 2002, a retail chain was reported to be running its wireless LAN without any form of encryption. The retailer responded by saying that its wireless LAN only handled its inventory application, so encryption was not needed. However, the open connection invites hackers to snoop around on the network to possibly get into confidential customer records or sensitive corporate information.

Internal Vulnerabilities

Because security risks for wireless LANs can come from the most malicious hackers as well as employees with the best intentions, threats to wireless LAN security can be broken into internal vulnerabilities and external threats.

Internal vulnerabilities are comprised of rogue deployments, insecure configurations, and accidental associations to neighboring wireless LANs.

Rogue WLANs

Rogue access points are a well-documented problem. In 2001 Gartner estimated that “at least 20 percent of enterprises already have rogue WLANs attached to their corporate networks.” Employees can easily hide their rogue access points to wired-side sniffers by simply setting the access point to duplicate the MAC address of the laptop – an easy and often mandatory configuration for a consumer-grade access point when installed to a home cable or DSL modem.

Other rogue deployments or unauthorized uses of wireless LANs can include ad hoc networks. These peer-to-peer connections between devices with WLAN cards do not require an access point or any form of authentication from other stations with which it connects. While ad hoc networks can be a convenient feature for users to transfer files between stations or connect to shared network printers, they present an inherent security risk where a station in ad hoc mode opens itself to a direct attack from a hacker who can download files from the victim’s station or use the authorized station as a conduit to the entire network.

Insecure Network Configurations

Many organizations secure their wireless LANs with virtual private networks and then mistakenly believe the network is bulletproof. While it takes a highly sophisticated hacker to break a VPN, a VPN can be like an iron door on a grass hut if the network is not properly configured. Why would a thief try to pick the lock of the iron door if he could easily break through the thin walls of the hut? All security holes – big and small – can be exploited.

By year-end 2002, 30 percent of enterprises will suffer serious security exposures from deploying WLANs without implementing the proper security.

– Gartner Group, August 2001

Insecure configurations represent a significant concern. Default settings that include default passwords, open broadcasts of SSIDs, weak or no encryption, and lack of authentication can open an access point to be a gateway to the greater network. Properly configured access points can be reconfigured by employees seeking greater operability or often reset to default settings upon a power surge or system failure.

Accidental Associations

Accidental associations between a station and a neighboring wireless LAN are just now being recognized as a security concern as enterprises confront the issue of

overlapping networks. Accidental associations are created when a neighboring company across the street or on adjacent floors of the building operates a wireless LAN that emanates a strong RF signal that bleeds over into your building space. The wireless LAN-friendly Windows XP operating system enables your wireless users to automatically associate and connect to the neighbor’s network without their knowledge.

A station connecting to a neighboring wireless LAN can divulge passwords or sensitive documents to anyone on the neighboring network. Accidental associations can even link the two companies’ networks together through this end user station as it bypasses all internal security and controls.

External Threats

The internal vulnerabilities previously described open the door for intruders and hackers to pose more serious threats. However, the most secure wireless LANs are not 100 percent safe from the continuously evolving external threats that include espionage, identity theft, and other attacks such as Denial-of-Service and Man-in-the-Middle attacks.

Eavesdropping & Espionage

Because wireless communication is broadcast over radio waves, eavesdroppers who merely listen to the airwaves can easily pick up unencrypted messages. Additionally, messages encrypted with the Wired Equivalent Privacy (WEP) security protocol can be decrypted with a little time and easily available hacking tools. These intruders put businesses at risk of exposing sensitive information to corporate espionage.

Identity Theft

The theft of an authorized user’s identity poses one the greatest threats. Service Set Identifiers (SSIDs) that act as crude passwords and Media Access Control (MAC) addresses that act as personal identification numbers are often used to verify that clients are authorized to connect with an access point. Because existing encryption standards are not foolproof, knowledgeable intruders can pick off authorized SSIDs and MAC addresses to connect to a wireless LAN as an authorized user with the ability to steal bandwidth, corrupt or download files, and wreak havoc on the entire network.

Evolving Attacks

More sophisticated attacks, such as Denial-of-Service and Man-in-the-Middle attacks, can shut down networks and compromise security of virtual private networks. This paper goes into greater detail describing how these attacks occur in the section *Emerging Attacks on WLANs*.

The Hacker's Wireless LAN Toolbox

Hackers – as well as white hat researchers – are notorious for quickly breaking the new security standards soon after the standards are released. Such is the case with the security standards for wireless LANs. This section provides a few examples of the hardware and freeware tools available on the Internet.

Available Freeware Tools

As mentioned in the introduction, new wireless LAN hacking tools are introduced every week and are widely available on the Internet for anyone to download. Rather than wait for a hacker to attack your network, security managers should familiarize themselves with tools to know what they have to defend themselves against. The table on this page gives a few examples of widely available freeware tools. Network security managers should become familiar with these hacking tools in order to know the dangers of each.

Antennas

To connect with wireless LANs from distances greater than a few hundred feet, sophisticated hackers use long-range antennas that are either commercially available or built easily with cans or cylinders found in a kitchen cupboard and can pick up 802.11 signals from up to 2,000 feet away. The intruders can be in the parking lot or completely out of site.

Breaking Encryption

The industry's initial encryption technology, WEP, was quickly broken by published tools WEPCrack and AirSnort, which exploit vulnerabilities in the WEP encryption algorithm. WEPCrack and AirSnort passively observe WLAN traffic until it collects enough data by which it recognizes repetitions and breaks the encryption key.

Breaking 802.1x Authentication

The next step in the evolution of wireless LAN security was the introduction of 802.1x for port-based

authentication. However, University of Maryland professor William Arbaugh published a research paper in February 2002 that demonstrated how the newly proposed security standard can be defeated. The IEEE is now working on a new standard, 802.1i, which is expected to be ratified within the next two years.

War Driving

To locate the physical presence of wireless LANs, hackers developed scanning and probing tools that introduced the concept of "war driving" – driving around a city in a car to discover unprotected wireless LANs. User-friendly Windows-based freeware tools, such as Netstumbler, probe the airwaves in search of access points that broadcasted their SSIDs and offer easy ways to find open networks. More advanced tools, such as Kismet, were then introduced on Linux platforms to passively monitor wireless traffic.

Both Netstumbler and Kismet work in tandem with a global positioning system (GPS) to map exact locations of the identified wireless LANs. These maps and data are posted on web sites such as www.wigle.net and www.wifinder.com where wireless freeloaders and other hackers can locate these open networks.

Emerging Attacks on WLANs

The development of effective wireless LAN security standards has been preceded by the evolution wireless-focused attacks that are becoming more sophisticated.

Attacks at DefCon

The growing number of attacks on wireless LANs is best seen in a study of wireless LAN activity at the DefCon X hacker convention in August 2002. AirDefense surveyed the wireless LAN at the Las Vegas convention for two hours and identified more than 10 previously undocumented wireless attacks from new creative ways in which hackers are learning to manipulate 802.11 protocols to launch new forms of Denial-of-Service

Tool	Web site	Description
NetStumbler	www.netstumbler.com	Freeware wireless access point identifier – listens for SSIDs & sends beacons as probes searching for access points
Kismet	www.kismetwireless.net	Freeware wireless sniffer and monitor – passively monitors wireless traffic & sorts data to identify SSIDs, MAC addresses, channels and connection speeds
Wellenreiter	http://packetstormsecurity.nl	Freeware WLAN discovery tool – Uses brute force to identify low traffic access points; hides your real MAC; integrates with GPS
THC-RUT	www.thehackerschoice.com	Freeware WLAN discovery tool – Uses brute force to identify low traffic access points; "your first knife on a foreign network"
Ethereal	www.ethereal.com	Freeware WLAN analyzer – interactively browse the capture data, viewing summary and detail information for all observed wireless traffic
WEPCrack	http://sourceforge.net/projects/wepcrack/	Freeware encryption breaker – Cracks 802.11 WEP encryption keys using the latest discovered weakness of RC4 key scheduling
AirSnort	http://airsnort.shmoo.com	Freeware encryption breaker – passively monitoring transmissions, computing the encryption key when enough packets have been gathered
HostAP	http://hostap.epitest.fi	Converts a WLAN station to function as an access point; (Available for WLAN cards that are based on Intersil's Prism2/2.5/3 chipset)

attacks, identity thefts, and Man-in-the-Middle attacks. During the two hours of monitoring the conference's wireless LAN, AirDefense identified 8 sanctioned access points, 35 rogue access points, and more than 800 different station addresses.

AirDefense's 802.11 security experts estimate that 200 to 300 of the station addresses were fakes because roughly 350 people were in the wireless LAN network room at a single time.

AirDefense discovered 115 peer-to-peer ad hoc networks and identified 123 stations that launched a total of 807 attacks during the two hours.

Among the 807 attacks:

- 490 were wireless probes from tools such as Netstumbler and Kismet, which were used to scan the network and determine who was most vulnerable to greater attacks;
- 190 were identity thefts, such as when MAC addresses and SSIDs were spoofed to assume the identity of another user;
- 100 were varying forms Denial-of-Service attacks that either (1) jammed the airwaves with noise to shut down an access point, (2) targeted specific stations by continually disconnecting them from an access point, or (3) forced stations to route their traffic through other stations that ultimately did not connect back to the network; and
- 27 attacks came from out-of-specification management frames where hackers launched attacks that exploited 802.11 protocols to take over other stations and control the network.

The wireless LAN at DefCon was probably the best place to learn about these new attacks and threats to wireless LANs because DefCon is one of few places where the focus is on breaking things. Enterprises should be aware of these threats and learn what they can do to combat them.

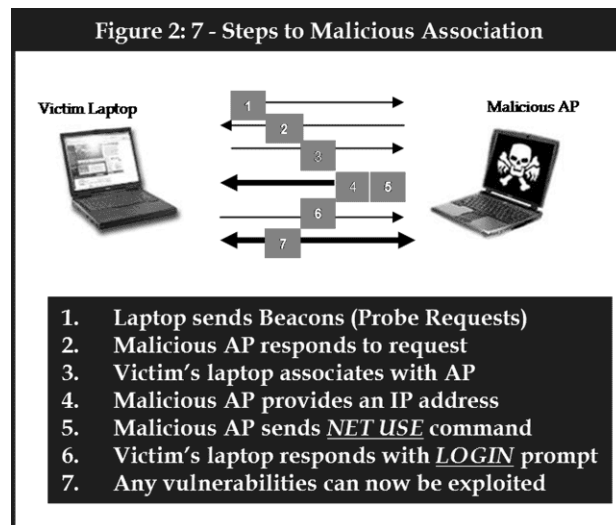
– **Pete Lindstrom, Spire Security, September 2002**

Of the more than 10 new types of attacks identified by AirDefense, the company's 802.11 security experts determined that many were new forms of Denial-of-Service attacks but an apparent danger came from the growing number of ways in which hackers have learned to abuse 802.11 protocols.

The following section outlines four major attacks, which represent significant dangers to wireless LANs because they are published attacks that unsophisticated hackers can easily perform after downloading tools off the Internet.

Malicious Association

Using widely available tools, hackers can force unsuspecting stations to connect to an undesired 802.11 network or alter the configuration of the station to operate in ad-hoc networking mode. A hacker begins this attack by using freeware HostAP to convert the attacking station to operate as a functioning access point.



As the victim's station broadcasts a probe to associate with an access point, the hacker's new malicious access point responds to the victim's request for association and begins a connection between the two. After providing an IP address to the victim's workstation (if needed), the malicious access point can begin its attacks. The hacker – acting as an access point – can use a wealth of available hacking tools available that have been tested and proven in a wired environment. At this time, the hacker can exploit all vulnerabilities on the victim's laptop, which can include installing the HostAP firmware or any other laptop configuration or programmatic changes.

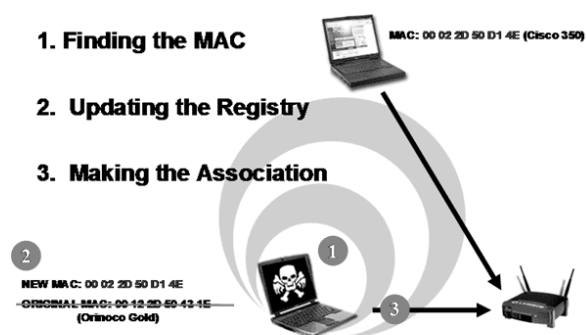
The malicious association attack shows that wireless LANs are subject to diversion and stations do not always know which network or access point they connect to. Stations can be tricked or forced to connect to a malicious access point. Even wireless LANs that have deployed VPNs are vulnerable to malicious associations. This attack does not try to break the VPN. Rather, it takes over the security-poor client.

Enterprises must monitor the airwaves of their wireless LAN to make sure their stations only connect to authorized access points and networks. Monitoring the network is the only way to know whom your stations connect to and which stations connect to your access points.

MAC Spoofing – Identity Theft

Many enterprises secure their wireless LAN with authentication based on an authorized list of MAC addresses. While this provides a low level of security for smaller deployments, MAC addresses were never intended to be used in this manner. Any user can easily change the MAC address of a station or access point to change its “identity” and defeat MAC address-based authentication.

Figure 3: MAC Spoofing of an Authorized Station



Software tools, such as Kismet or Ethereal, are available for hackers to easily pick off the MAC addresses of an authorized user. The hacker can then assume the identity of that user by asserting the stolen MAC address as his own. The hacker then connects to the wireless LAN as an authorized user.

By monitoring the airwaves of their wireless LAN, enterprises are able to detect MAC spoofing by identifying when more than one MAC address are simultaneously on the network. Wireless LAN intrusion detection systems can also identify when a MAC address is spoofed by analyzing the vendor “fingerprints” of the wireless LAN card where by the IDS can see when, as an example, an Orinoco wireless LAN card connects to the network using MAC address of a Cisco WLAN card.

Man-in-the-Middle Attacks

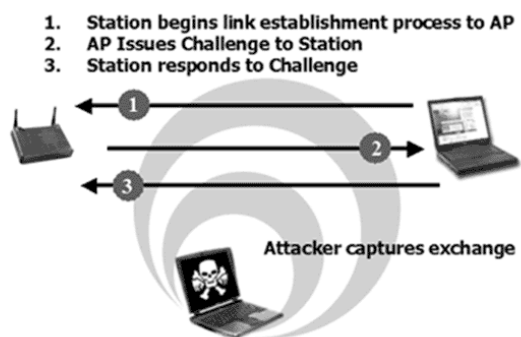
As one of the more sophisticated attacks, a Man-in-the-Middle attack can break a secure VPN connection between an authorized station and an access point. By inserting a malicious station between the victim station and the access point, the hacker becomes the “man in the middle” as he tricks the station into believing he is the access point and tricks the access point into believing he is the authorized station.

This attack preys upon a CHAP implementation to randomly force a connected station to re-authenticate with the access point. The station must respond to a

random challenge from the access point, and the access point must respond to a successful challenge response with a success packet.

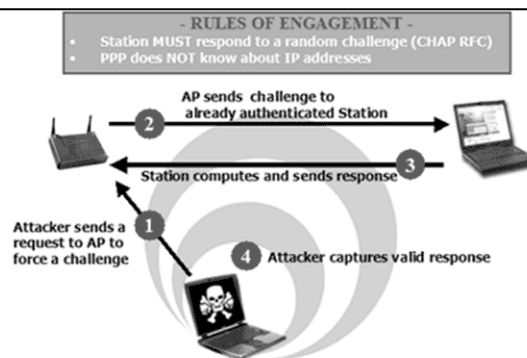
To begin this attack, the hacker passively observes the station as it connects to the access point, and the hacker collects the authentication information, including the username, server name, client and server IP address, the ID used to compute the response, and the challenge and associate response. (See Figure 4)

Figure 4: VPN Attack – Link Establishment, Challenge, Response



The hacker then tries to associate with the access point by sending a request that appears to be coming from the authenticated station. The access point sends the VPN challenge to the authenticated station, which computes the required authentic response, and sends the response to the access point. The hacker observes the valid response. (See Figure 5)

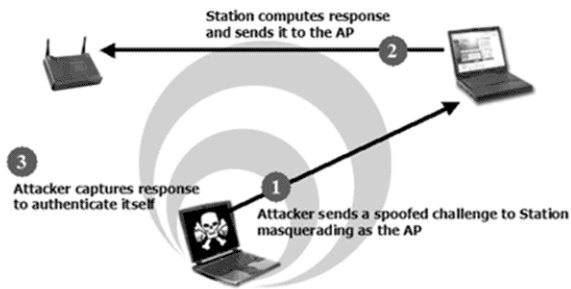
Figure 5: VPN Attack – Mounting the assault



The hacker then acts as the access point in presenting a challenge to the authorized station. The station computes the appropriate response, which is sent to the access point. The access point then sends the station a success packet with an imbedded sequence number. Both are

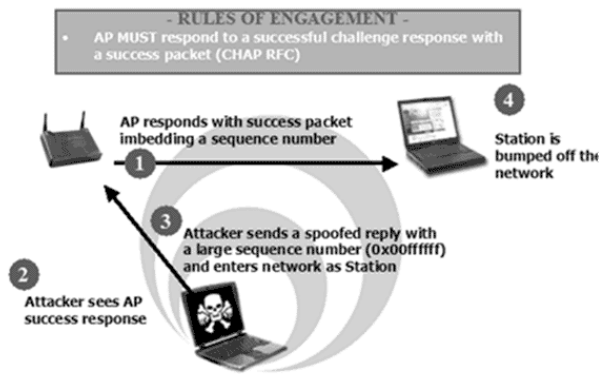
captured by the hacker. After capturing all this data, the hacker then has what he needs to complete the attack and defeat the VPN. (See Figure 6)

Figure 6: VPN Attack – Getting in the Middle



The hacker sends a spoofed reply with large sequence number, which bumps the victim’s station off the network and keeps it from re-associating. The hacker then enters the network as the authorized station. (See Figure 7)

Figure 7: VPN Attack – Entering the Network



Only 24x7 monitoring and a highly capable wireless IDS can detect this type of attack on a wireless LAN. An effective security solution must first keep a constant watch over the wireless LAN while it analyzes the activity it observes. A wireless IDS should be able to detect this type of attack based on its signature as well as the simultaneous use a single MAC address and user name by both the authorized station and the hacker.

Denial-of-Service Attacks

Every network and security managers fears the downtime and loss of productivity from a crippling Denial-of-Service attack. In the wireless world, this damaging attack can come from any direction, and the most basic

variations of DoS attacks can be just as worrisome as the most sophisticated.

Because 802.11b wireless LANs operate on the unregulated 2.4 GHz radio frequency that is also used by microwave ovens, baby monitors, and cordless telephones, commonly available consumer products can give hackers the tools for a simple and extremely damaging Denial-of-Service attack. Unleashing large amounts of noise from these other devices can jam the airwaves and shut down a wireless LAN.

Hackers can launch more sophisticated Denial-of-Service attacks by configuring a station to operate as an access point. As an access point, the hacker can flood the airwaves with persistent “disassociate” commands that force all stations within range to disconnect from the wireless LAN. In another variation, the hacker’s malicious access point broadcasts periodic disassociate commands every few minutes that causes a situation where stations are continually kicked off the network, reconnected, and kicked off again.

In addition to malicious disassociation attacks, hackers are now using abusing the Extensible Authentication Protocol (EAP) to launch Denial-of-Service attacks. “The Unofficial 802.11 Security Web Page” at <http://www.drizzle.com/~aboba/IEEE/> lists six forms of Denial-of Service attacks from various ways hackers can manipulate EAP protocols by targeting wireless stations and access points with log-off commands, start commands, premature successful connection messages, failure messages, and other modifications of the EAP protocol.

Newly developing Denial-of-Service attacks exploit improperly configured wireless LANs or rogue access points to target the entire enterprise network. When an access point is attached to an unfiltered segment of the enterprise network, the access point broadcasts “Spanning Tree” (802.1D) packets. This opens the door to attacks that take down all wireless equipment as well as spur a **meltdown of the entire internal networking infrastructure** – hubs, routers, switches, etc. – that are connected behind the WLAN access point.

In normal operation, the Spanning Tree algorithm ensures the existence of a loop-free Ethernet topology in networks that contain parallel bridges and multiple Ethernet segments. A loop occurs when there are alternate routes between hosts. If a loop exists in an extended network, bridges may forward traffic indefinitely to false or wrong Ethernet hosts, which can result in increased traffic and degradation in network performance to a point where they no longer will respond or operate.

A hacker can launch a Denial-of-Service attack by intentionally inserting this loop on the network. The hacker goes through the wireless LAN to maliciously replay an altered Spanning Tree session back to the enterprise.

A rogue sniffer can initiate this by attack echoing a manipulated replay Spanning Tree session back to the wireless LAN access point, which in turn echoes the manipulated Spanning Tree packets to other internal hosts with a devastating domino effect. Spanning Tree attacks will typically render the intelligent hubs, bridges, routers, and switches completely inoperative and usually require rebooting or reconfiguration of these devices to make them operative again.

Any rogue access point plugged into a port on a hub or into a switch or router that is not filtered by a firewall can open a network to this most damaging Denial-of-Service attack. AirDefense has found that nearly 1 out of 20 wireless LANs surveyed are vulnerable to this form of Denial-of-Service attack from rogue access points and improperly configure wireless LANs.

The AirDefense Solution

AirDefense provides the industry's only security appliance for WLANs to discover WLAN vulnerabilities, enforce security policies, and detect and respond to intruders. AirDefense's patent-pending technology integrates multi-dimensional intrusion detection with stateful monitoring to ensure security across enterprise 802.11 WLANs.

More simply put, AirDefense is a wireless LAN intrusion protection and management system that discovers network vulnerabilities, detects and protects a WLAN from intruders and attacks, and assists in the management of a WLAN.

AirDefense: (i) Discovers vulnerabilities and threats – such as rogue APs and ad hoc networks – as they happen; (ii) Secures a WLAN by detecting intruders and attacks and eliminating those threats; and (iii) Provides a robust WLAN management functionality that allows users to understand their network, monitor network performance, and enforce network policies.

Remote Sensors & Server Appliances

The AirDefense solution consists of distributed sensors and server appliances. The remote sensors sit near 802.11 Access Points to monitor all WLAN activities and report back to the server appliance, which analyzes the traffic in real time.



The remote sensors:

- Are deployed near Access Points;
- Cover 40,000 square feet of typical office space
- Provide 24x7 monitoring of all WLAN activities;
- Capture wireless traffic from Access Points and stations;
- Report to a back-end server; and
- Are centrally managed.

The server appliances:

- Analyze traffic in real time;
- Discover WLANs and rogue deployments;
- Detect intrusions and impending threats;
- Includes ActiveDefense technologies to respond to attacks, network misconfigurations, and policy violations;
- Enforce WLAN policies;
- Monitor WLAN performance and troubleshoot network issues;
- Offer a secure web-based interface; and
- Provide comprehensive reporting.

AirDefense's Differentiating Technology

AirDefense was developed based on sophisticated, patent-pending data capture and analysis technology. With its State-Analysis Engine™, AirDefense provides 24x7, real-time monitoring of all WLAN traffic and correlates the data among its Multi-Dimensional Detection Engine™ to identify security risks.

AirDefense is the only WLAN security solution to provide stateful monitoring of the airwaves. Stateful means that AirDefense provides continuous monitoring of the "state" of communication between all Access Points and stations transmitting on the airwaves. With a minute-by-minute account of all WLAN traffic, intruders are immediately recognized, attacks are quickly detected, and appropriate measures can be taken to secure the network. The State-Analysis Engine enables AirDefense

to track and control the flow of communication on an enterprise WLAN.

AirDefense built its patent-pending Multi-Dimensional Detection Engine as a WLAN intrusion detection system based upon multiple detection technologies exclusively designed for Layer 1 and Layer 2 of 802.11 protocols.

Traditional intrusion detection systems are plagued by false positives because they rely on a single detection technology – mostly attack signatures. AirDefense has developed its Multi-Dimensional Detection Engine as a comprehensive WLAN intrusion detection system that integrates multiple detection technologies that correlate data to recognize real threats and reduce false positives. The patent-pending State-Analysis Engine coordinates inputs and the multi-dimensional detection engine analyzes threats to identify security breaches based on:

- Signature analysis
- Policy compliance
- Protocol assessment
- Statistically anomalous behavior.

ActiveDefense technology allows AirDefense to integrate with enterprise WLANs and respond to attacks, network misconfigurations, and policy violations. Once an intruder or attack is identified, AirDefense communicates with the Access Point to terminate the malicious connection. If an access point is identified as violating a configuration policy, such as mandated encryption, AirDefense reconfigures the Access Point to only allow encrypted traffic to flow through WLAN.

By monitoring wireless device traffic, AirDefense can isolate, prevent, or mitigate network intrusions and subsequent downtime.

– InfoWorld, March 2003

Combating Wireless Threats & Attacks

AirDefense secures wireless LANs with 24x7 stateful monitoring of all wireless traffic and advanced intrusion detection. The State Analysis Engine and Multi-Dimensional Detection Engine power AirDefense to secure wireless LANs against the threats and attacks mentioned in this paper

Combating Rogue WLANs & Insecure Network Configurations

By monitoring the airwaves for all wireless LAN traffic, AirDefense identifies rogue access points and network vulnerabilities as soon as they arise. Freeware, such as Netstumbler and Kismet, and other commercial scanners can survey the airwaves for rogue access points and some network vulnerabilities. However, this process requires a network administrator to physically walk through the wireless LAN coverage area for the scanner

to pick up data that the network administrator interprets to identify all access points and wireless LAN traffic. While this process requires the physical presence and valuable time of a network manager, the effectiveness is limited because it only samples the airwaves for threats. New rogue access points and other vulnerabilities can arise after a scan and will not be detected until the next time a network administrator surveys the network.

Only AirDefense provides 24x7 monitoring of the airwaves to provide and identify:

- Site Surveys
- Rogue Deployments
- Unauthorized Use
- Security Vulnerabilities.

Combating Malicious & Accidental Associations

By monitoring all wireless LAN traffic, AirDefense identifies all wireless LAN stations and access points in the area. AirDefense then analyzes the traffic to ensure that the stations and laptops are only associating with authorized users. Network security managers are alerted to the intruders or accidental associations, and AirDefense has the ability to disconnect stations from unauthorized access points and disconnect unauthorized stations from network access points.

Combating MAC Spoofing & Identity Theft

AirDefense monitors the airwaves of wireless LANs and detects MAC spoofing by identifying when more than one MAC address are simultaneously on the network. AirDefense also identifies when a MAC address is spoofed by analyzing the vendor “fingerprints” of the wireless LAN cards connecting to the network. Once an intruder is identified, AirDefense can disconnect the unauthorized station.

Combating Man-in-the-Middle Attacks

A VPN with strong mutual authentication can guard against many Man-in-the-Middle attacks. AirDefense protects a wireless LAN against all Man-in-the-Middle attacks by first identifying the attack as it occurs, then alerting security managers of the attack, and finally disconnecting the attacker from the network.

AirDefense identifies the attack based on known attack signatures and protocol abuses whereby the hacker forces an access point and station to alter the established protocols for association and authentication.

Combating Denial-of-Service Attacks

In monitoring the health of a wireless LAN, AirDefense alerts network security managers to Denial-of-Service attacks and can combat many forms of DoS attacks by launching a reverse attack on the hacker.

About AirDefense, Inc.

AirDefense is a thought leader and innovator of wireless LAN security and operational support solutions. Founded in 2001, AirDefense pioneered the concept of 24x7 monitoring of the airwaves and now provides the most advanced solutions for rogue WLAN detection, policy enforcement, intrusion protection and monitoring the health of wireless LANs. As a key element of wireless LAN security, AirDefense complements wireless VPNs, encryption and authentication. Based on a secure appliance and remote sensors, AirDefense solutions scale to support single offices, corporate campuses or hundreds of locations. Blue chip companies and government agencies rely upon AirDefense solutions to secure and manage wireless LANs around the globe.

For more information or feedback on this white paper, please contact:

AirDefense, Inc.
11475 Great Oaks Way
Suite 200
Alpharetta, GA 30022
www.AirDefense.net
phone: 770.663.8115
email: info@airdefense.NET