AirDefense™

WHITE PAPER

Wireless LANs: Is My Enterprise At Risk?

Wireless LANs: Is My Enterprise At Risk?

The objective of this white paper is to provide an overall understanding of the risks associated with wireless LANs. The white paper also includes an overview of the inherent properties of wireless LANs and what makes them different from wired networks. The paper concludes with a list of recently published articles on real-life breaches and incidents illustrating the need for proactive measures to mitigate wireless security risks.

Wireless technology is exploding in popularity. Businesses are not only migrating to wireless networking, they are steadily integrating wireless technology and associated components into their wired infrastructure. The demand for wireless access to LANs is fueled by the growth of mobile computing devices, such as laptops and personal digital assistants, and a desire by users for continual connections to the network without having to "plug in."

> ***"Wireless LANs are the major wireless security problem facing businesses through 2008."***
> ***Gartner, 2004***

Like most innovative technologies, using wireless LANs poses both opportunities and risks. The wireless explosion has given momentum to a new generation of hackers who specialize in inventing and deploying innovative methods of hijacking wireless communications, and in using the wireless network to breach the wired infrastructure. In fact, hackers have never had it so easy.

1. What Makes Wireless LANs Different?

Shared, Uncontrolled Medium

Traditional wired networks use cables to transfer information. Cables are a controlled medium, protected by the buildings that enclose them. External traffic that enters a wired network is policed by a firewall and intrusion-protection technologies. To gain access to a wired network, an intruder or hacker must bypass the physical security of the building or breach the firewall.

Wireless networks, on the other hand, use the air space to transfer information. The air space is an uncontrolled and shared medium—it lacks the equivalent physical control of its wired counterpart. Once a user connects a wireless access point into the network, its signals can travel through the walls, ceilings, and windows of the building. This renders the entire network accessible from another floor of the building, from an adjoining building, from the parking lot, or from across the street. Radio signals from a single wireless access point can travel up to thousands of feet outside of the building. Additionally, wireless devices share the airspace. Any wireless device in the network can "see" all the traffic of all other wireless devices in the network.

Self-Deploying and Transient

Wireless devices are easy and relatively inexpensive to deploy, and completely mobile. Most laptops on the market today are wireless-ready. Older devices are easily converted to wireless by adding a wireless card and software. A stand-alone access point (AP) and a wireless card cost under $100.00 each. Alternately, a laptop can be easily converted into an AP. Well-intentioned employees, consultants, and contractors who install their own wireless stations and APs without regard to proper security configuration requirements pose a serious threat to the enterprise.

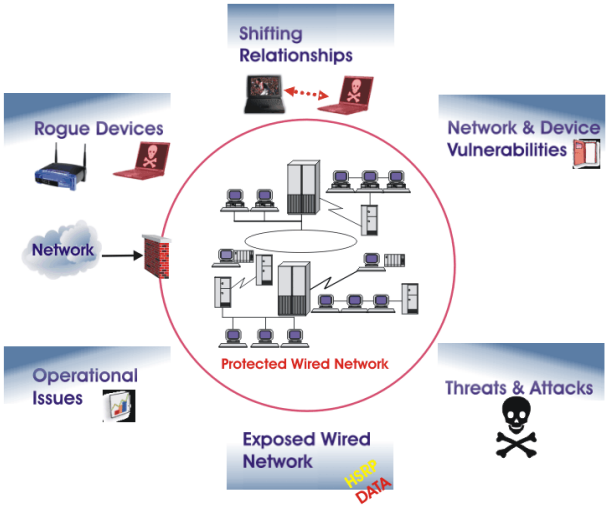
Of even more concern is the mobility of the devices connecting to wireless LANs and the increased exposure this introduces to the internal network. Wireless devices can come and go in the enterprise unnoticed, and can be located *anywhere*.

Easy to Attack

Because wireless communications are broadcast over the shared radio waves, they are easy for hackers to attack. The only physical boundary a wireless signal has is the strength of its own signal. An attacking hacker can "port" into your wireless network from any nearby location—a street, a car, nearby buildings, a park, etc. In short, a kid on a bicycle with a PDA in his or her shirt pocket could be running a reconnaissance on your wireless network right now. The advent of readily-available software "hacker's tools" is increasing the risks of using the shared air space. These enable more sophisticated hackers to "sniff" data and applications, intercept traffic, and break both encryption and authentication. For more information on hacker's tools, see the AirDefense White Paper *"What Hacker's Know That You Don't."*

2. The Six Risks of Using Wireless LANs

Wireless introduces new security challenges. The same wireless technologies that operate without the physical and logical barriers of their wired counterparts, increase user flexibility, boost productivity, and lower network costs, can also expose network-based assets to considerable risk. The following describes the six greatest threats to WLAN security.



Risk One—Rogue Devices

Unauthorized rogue devices, particularly rogue APs, are the most daunting challenge created by wireless technology. The rapid proliferation of rogue devices poses a serious threat to the enterprise. According to analysts, there are tens of thousands of rogue devices in enterprise networks nationwide.

A rogue AP can be a soft AP, hardware AP, laptop, scanner, projector, or other device. Rogues provide an open entry point to the enterprise's entire network infrastructure, bypassing all existing security measures.

Risk Two—Shifting Relationships

Wireless devices have constantly shifting network relationships with other wireless devices. Accidental association takes place when a wireless laptop running the LAN-friendly Windows® XP or a misconfigured client automatically associates and connects to a user station in a neighboring network. This enables intruders to connect to innocent user's computers often without their knowledge, compromise sensitive documents on the user station, and expose it to even further exploitation. This danger is compounded if the station is connected to a wired network, which is also now accessible.

"Any U.S. enterprise, branch office, plant or store with more than 50 employees probably has one or more rogue APs."
Thor Sigvaldson, PwC Consulting

Ad hoc networks are peer-to-peer connections between devices with wireless LAN cards that do not require an access point or any form of authentication from other user stations. While these ad-hoc networks can be convenient for transferring files between stations or to connect to network printers, since they lack security, they enable hackers to easily compromise an innocent user's station or laptop.

Risk Three—Network & Device Vulnerabilities

Insecure wireless LAN devices, such as access points and user stations, can seriously compromise both the wireless network and the wired network. Hackers target insecure devices, using specialized tools to break encryption and authentication.

"Through 2006, 70 percent of successful wireless local area network (WLAN) attacks will be because of the misconfiguration of WLAN access points (APs) and client software."
Gartner, 2004

AP Misconfigurations

A single misconfigured access point can severely compromise the security of the enterprise wireless network. The default settings of most access points do not include authentication or encryption, and this factor, combined with the inexpensive cost of access points, makes centralized configuration control of access points very difficult. Individuals within the enterprise can set up access points without the knowledge of IT groups, with a high likelihood that most of these will be improperly

configured. It is these rogue access points that give hackers an open door to the wireless and wired internal network.

Wireless Station Misconfigurations

Misconfigured wireless user stations pose even a bigger risk to the security of the enterprise than do misconfigured access points. These devices can easily come and go in the enterprise. They often have no security configuration or are using an insufficient default configuration. Hackers can use any insecure wireless station as a launch pad to breach the network.

Breaking Encryption

Hackers use specialized encryption-breaking tools to crack the WEP encryption standard (see Sophisticated Tools in Risk Four). These tools are readily available, and inexpensive. They exploit vulnerabilities in the WEP encryption algorithm by passively observing wireless LAN traffic until they collect enough data to recognize the pattern and use the information to break the encryption key. Some tools minimize the time needed to crack long WEP keys from days to hours by using a traffic injection technique to create large amounts of traffic for key recovery.

Risk Four—Threats & Attacks

Wireless networks introduce multiple venues for attack and penetration that are either much more difficult or completely impossible to execute with a standard, wired network.

Reconnaissance

Traditional attacks require a reconnaissance phase, in which the hacker sees which systems are available for enumeration and attack. To perform the reconnaissance, the hacker uses wireless LAN scan tools such as NetStumbler, Wellenreiter, and Windows XP.

Identity Theft

The theft of an authorized user's identity is a serious threat to wireless networks. Even though SSIDs and media access control (MAC) addresses act as personal identification numbers for verifying the identity of authorized clients, existing encryption standards are not foolproof. Knowledgeable hackers can pick off authorized SSIDs and MAC addresses and steal bandwidth, corrupt or download files, and wreak havoc on the entire network. There is a misconception that identity theft is only feasible if the MAC address is used for authentication, and that 802.1x-based authentication schemes such as LEAP are totally safe. Cracking LEAP to steal identity has become easy with sophisticated hacker's tools. Other authentication schemes, such as EAP-TLS and PEAP, may require more sophisticated attacks that exploit other known vulnerabilities in wired side authentication schemes.

Various Types of Attack Tools

- Encryption-breaking tools
- Authentication-breaking tools
- Denial-of-Service Tools
- Vulnerability Scanners

Denial-Of-Service

The objective of any denial-of-service (DoS) attack is to prevent users from accessing network resources to deny them service. The usual methods of triggering DoS attacks are to flood a network with degenerate or faulty packets, crowding out legitimate traffic and causing systems not to respond.

Sophisticated Attack Tools

The tools that hackers use are widely available for free on the Internet, and new tools are introduced every week. These tools enable hackers to break encryption and authentication, analyze protocols, sniff the airspace, and capture traffic, including IP addresses, user names and passwords.

Encryption-breaking tools such as WEPWedgie, WEPCrack, WepAttack, BSD-Airtools, and AirSnort enable hackers to decrypt messages that use WEP.

- Authentication-breaking tools such as ASLEAP and THC-LEAPCracker enable hackers to break or compromise variations of the port-based authentication protocols for 802.1x wireless, such as LEAP and PEAP. Using these, the hacker can capture authentication credentials.
- Tools such as WLANjack and hunter_killer enable hackers to launch DoS attacks.
- A Windows vulnerability scanner such as Nessus enables hackers to scan for vulnerable devices, such as user stations and access points, which are attached to the wireless network.

Risk Five—Exposure of the Wired Network

Most enterprise wireless LANs connect back to a wired network at some point. Hackers can use any insecure wireless station as a launch pad to breach the network. Additionally, misconfigured access points can act as a bridge to the wired network, sending multicast, wired data, and credentials into the air, where they can be intercepted by intruders and hackers on the wireless side of the network. Also, enterprises that use routing protocols, such as HSRP (hot standby routing protocol), can fall prey to hackers doing wireless reconnaissance for topography information about the wired network. These types of protocols reveal information that can enable a hacker to do traffic analysis of the enterprise, such as the devices in use, MAC addresses, IP addresses, and traffic routes.

Risk Six—Operational Issues

Wireless LANs have operational issues that can compromise the usability of the wireless network, issues that impact availability, performance, security, and cost. To alleviate these issues, wireless LANs require effective operational support mechanisms to run smoothly. Support for wireless LANs cannot depend on traditional wire-based support tools, but instead, must have tools that monitor performance, diagnose faults, and monitor for network use and misuse.

Off-Hours Activity

Because wireless devices are not subject to the confines of a wired network, they can be used anywhere, and at any time of day. For this reason, many enterprises limit wireless usage to set office hours, even going so far as to turn off access points during off hours. In this way, all wireless traffic that takes place during off hours is automatically deemed suspicious.

Data Rates

Access points that advertise slow and unsafe data rates can invite a security breach. If properly deployed, enterprise 802.11b wireless LANs should serve its user stations with a connection rate of 5.5 Mbps or 11 Mbps. The access points then are configured to only allow for these desired data rates. However, an access point that allows users to connect at the slower 1 Mbps and 2 Mbps speeds indicates degraded network performance or potential suspicious activity. A connection of 1-Mbps on a properly deployed network indicates potential suspicious activity from someone in the parking lot or down the street with an antenna.

Interference

Because wireless LANs use radio waves, conditions and events can change how the WLAN operates. An example is RF interference, which can cause inoperability in the wireless network and excessive retransmissions of data. The source of RF interference can be another electronic device operating in the area. WLANs have limited transmission capacity that is shared between all users associated to a single access point. Hackers can easily launch a denial of service attack on such limited resources.

Rogue APs or other devices can interfere with the operation of “legitimate” devices, and in addition, provide hackers with an insecure interface to the corporate network. A hacker may try to access network resources by intentionally installing a rogue AP to intercept sensitive information or fake a connection to a legitimate AP. In addition, somebody wanting to restrict usage of the wireless LAN could try jamming an AP with strong radio signals.

Connectivity

A number of factors can cause wireless connections to degrade or to drop off entirely. Wireless networks can experience a loss of performance and users can have access problems when wireless signals encounter natural or manmade obstructions between the user and the AP, or when the user is a great distance from the AP. Throughput issues can cause delays for users, for example, when there is a number of users connected to an AP at the same time. A malfunctioning or inoperative AP can prevent or limit access to the network.

3. Are Wireless Networks really at Risk?

Published Security Breaches

According to a November, 2003 survey by PricewaterhouseCoopers, 46 percent of companies and agencies who have wireless networks have been victims of a security breach. Of these, 83 percent

reported a monetary loss. Any wireless device or unauthorized access point creates an on-ramp to the entire wireless and wired networks. Unless properly configured, secured and monitored, these wireless devices and networks are dangerous to the entire organization. The following list of recently published articles illustrates the real need for proactive measures to mitigate wireless security risks. Each concerns a prominent company or agency that was victim to security breaches to their wireless network, and in some cases, their wired company network.

> ***"By 2005, 60 percent of security breach incident costs incurred by businesses will be financially or politically motivated."***
> ***Gartner***

A Major National Retailer

Detroit Free Press—The Detroit Free Press reported in 2003 that a major national retailer's customer credit card numbers and other proprietary information were compromised by three men working from a one store's parking lot. According to the article, federal prosecutors stated that the men repeatedly hacked into the unsuspecting chain's national computer network by logging onto a user account over the wireless network. Once in the system, the hackers gained access to the chain stores in six states, plus the headquarters' system, where they accessed credit card numbers and other proprietary information. The article further explained that statements made by the three men indicated that they "stumbled across the chain's unsecured wireless network while driving around with laptop computers looking for wireless internet connections," a concept known in wireless technology as *war driving*.

As reported to the Detroit Free Press, prosecutors said the men used the insecure wireless network to route through the chain's corporate data center and connect to the local networks at the chain's stores around the country. At two of the stores, they modified a propriety piece of software that the chain uses to process credit card transactions, building in a virtual wiretap that would store customers' credit card numbers for later retrieval and use.

In the article, representatives of the chain told prosecutors their wireless LAN system was installed to allow scanners and telephones to connect to the store's network without the burden of cables. When asked why they were not running encryption, the representatives stated that their wireless LAN only handled company inventory applications that did not require encryption.

A Major Electronics Retailer

Addison-Wesley—Customer credit cards and credit data was compromised in 2002 by hackers working from the parking lot of a national electronics retailer. According to an article published in the Addison-Wesley online series by e-commerce consultant Frank Fiore, the retailer used a sophisticated wireless network that enabled their cash registers to beam information, including customer credit card numbers, to a central computer for processing elsewhere in the store. The wireless beams were easily intercepted by hackers.

According to Fiore, "What many organizations fail to understand is that wireless signals emanating from their network are not confined to their offices, or even their building. Wireless signals can easily pass through office ceilings, walls, and floors."

A California Public School District

The Palo Alto Weekly—Using a laptop with a wireless card outside of a school district's main office, reporters for the Palo Alto Weekly were able to access highly sensitive computer files from a Northern California school district. According to the 2003 Weekly article, the school district's unprotected wireless LAN allowed full unauthorized access to sensitive files and also enabled hackers to upload their own files into the servers. "This clearly illustrates the hazards of an open wireless network if proper security measures are not enacted," stated the Weekly. The Weekly was able to gain access to files containing grades, home phone numbers and addresses, emergency medical information, full color photos, and psychological evaluations of each student, which according to the article, is a breach of federal law governing distribution of students' education records. The Weekly further reported that it was able to open files in the 40-server wide-area-network (WAN) as easily as opening a Microsoft Word file.

In the article, a network administrator for the school district admitted to the Weekly that security was an afterthought when the first open wireless networks were installed in district schools. "The district was more interested in equipment issues than securing information," he said.

A County Court in Texas

Houston Chronicle—The Houston Chronicle reported in 2002 that a Houston computer security analyst successfully hacked into a local county court wireless LAN to demonstrate the insecurity of the county courts. According to the report, the analyst was able to easily access information filed by the clerk of courts by using only a laptop computer and wireless card, an intrusion that reportedly cost the county $5,000.00 to clean up.

A North Carolina Medical Consulting Firm

WRAL-TV—Raleigh, North Carolina television station WRAL-TV recently reported that an information security consultant broke into the computer system of a local medical consulting firm and illegally accessed information of hundreds of patients, including checks and insurance forms.

A Major International Airport

KUSA-TV—According to a report by Denver, Colorado television station KUSA-TV, the new wireless internet service of a Colorado international airport, "the first *hotspot* of its kind," is completely unprotected and allows full access to the laptops of anyone using the service. According to KUSA-TV, once a passenger or visitor is connected to the wireless internet service, private information is no longer private. Citing one example, the station was able to obtain a passenger's password, cell phone number, social security number, visa card number and expiration date, and email. The passenger, who had simply used AT&T wireless to log online to check email, assumed the information was encrypted. Two computer security analysts who were also interviewed were able to see what other travelers were doing with their computers, to read their email, access their confidential information, and even access the employee names, titles, work orders, and flight times of a private air carrier. "The sad thing is, it's preventable," said one of the analysts.

According to KUSA-TV, when told about the security issues, a spokesperson for AT&T Wireless stated that "AT&T cannot protect data on a public system. Nothing is protected or confidential."

Enterprises in a Large Midwestern City

WCCO-TV—War-walking through downtown Minneapolis with security consultants, television station WCCO-TV reported that the wireless and wired networks of a number of prominent businesses and institutions, including a state university system, were insecure and fully accessible to anyone *armed* with a wireless laptop and some inexpensive, easily obtained hacker's tools. According to WCCO-TV, wireless hacking represents a new age of cyber crime. WCCO-TV reported that "Breaking into vulnerable companies gives hackers all the connectivity of someone who is sitting at a desk in the office, using their computer for work. By using inexpensive software for sale at an electronics stores or online, a hacker can crack the security of any unprotected company." The security consultants in the report demonstrated that once in the network, the hacker can use the unsuspecting user's computer to access an entire hard drive, steal the user's identity, access the internet, use email, or even use the wireless network to take control of another wireless network. They pointed out that in the wireless world, messages, credit card theft, harassment, fraud, or terrorism are not traceable. At another university facility, the WCCO-TV war-walkers were able to intercept communications, impersonate people, find student grades, and generally, watch all wireless traffic. The consultants cited "no password protection" as the most common reason that hackers are able to penetrate wireless networks. The companies that were the subject of this report refused comment. According to the report, the university shut down its wireless system until appropriate security could be implemented.

Conclusion

The benefits of wireless LANs are undeniable but the risks introduced by them are exponentially increasing. There are over tens of millions of new Wi-Fi devices shipped each year thereby increasing the number of potential points of access/ breach. The implications of these self-deploying, transient wireless networks make them dangerous to all organizations, regardless of their WLAN deployment status. Also these risks are not only restricted to the network edge but directly impact the wired corporate backbone.

But it is possible to have iron-clad protection for wireless networks and make them risk-free. The best way for organizations to fortify their wireless networks is to use a layered approach to security mirroring the security of wired networks. This layered approach includes:

- Locking down the wireless LAN's perimeter (both access points & wireless-enabled devices)
- Securing communication across the wireless LAN (authentication, encryption & VPNs)
- Continuously monitoring network traffic (24x7 Real-time Monitoring)

By continuously monitoring all wireless activity for rogue devices, threats and violations of configuration, usage and security policy, organizations can secure their entire corporate backbone. The monitoring solution should be able to recognize impending threats from network interference,

unknown stations scanning the network and the use of hacking reconnaissance tools. It should be able to enforce usage policies, such as mandatory encryption, to ensure that all traffic, including enterprise information assets, is fully protected. It should also detect and disconnect intruders who attempt to access an enterprise WLAN to steal confidential data or corrupt sensitive information.

About AirDefense

AirDefense, the market leader in anywhere, anytime wireless security and monitoring, is trusted by more Fortune 500 companies, healthcare organizations and high-security government agencies for enterprise wireless protection than any other wireless security provider. Ranked among *Red Herring*'s Top 100 Private Companies in North America, AirDefense products provide the most advanced solutions for rogue wireless detection, policy enforcement and intrusion prevention, both inside and outside an organization's physical locations and wired networks. Common Criteria-certified, AirDefense enterprise-class products scale to support single offices as well as organizations with hundreds of locations around the globe.

AirDefense Enterprise, the flagship product, is a wireless intrusion prevention system that monitors the airwaves 24x7 and provides the most advanced solution for rogue detection and mitigation, intrusion detection, policy monitoring and compliance, automated protection, forensic and incident analysis and remote troubleshooting. As a key layer of security, AirDefense Enterprise complements wireless VPNs, encryption and authentication. Using a monitoring architecture of distributed smart sensors and a secure server appliance, the AirDefense Enterprise system provides the most comprehensive detection of all threats and intrusions. Unlike any other solution on the market, AirDefense Enterprise analyzes existing and day zero threats in real time against historical data to more accurately detect threats and anomalous behavior originating inside or outside the organization. The system automatically responds to threats according to appropriate business process and compliance requirements on both wireless and wired networks, making AirDefense Enterprise the industry's most secure and cost-effective wireless intrusion prevention and troubleshooting solution.

AirDefense Personal, the industry's first end-point security solution, provides uninterrupted protection for all mobile employees and their enterprise wireless assets, regardless of location – at work, home, airports or other wireless hotspots. Policy profiles are defined centrally on AirDefense Enterprise and automatically downloaded to each mobile user. If threats are discovered, AirDefense Personal notifies the user and sends the alerts to AirDefense Enterprise for central reporting and notification. This unique solution allows the network administrator to enforce corporate policies and provide complete protection for the mobile workforce, regardless of location.

The **AirDefense InSite Suite** is a collection of powerful tools available today for network architects to design, install, maintain and troubleshoot wireless networks. Tools included in the suite are: **AirDefense Mobile**, complementary to AirDefense Enterprise allows administrators to perform wireless assessments, security audits, locate and manage rogues. **AirDefense Architect** provides complete design and 3D RF simulation of wireless LANs based on building-specific environments. **AirDefense Survey** provides real-time, in-the-field measurements of Wi-Fi RF environments for site-specific surveys.

For more information or feedback on this white paper, please contact info@airdefense.net or call us at 770.663.8115. ***All trademarks are the property of their respective owners.***