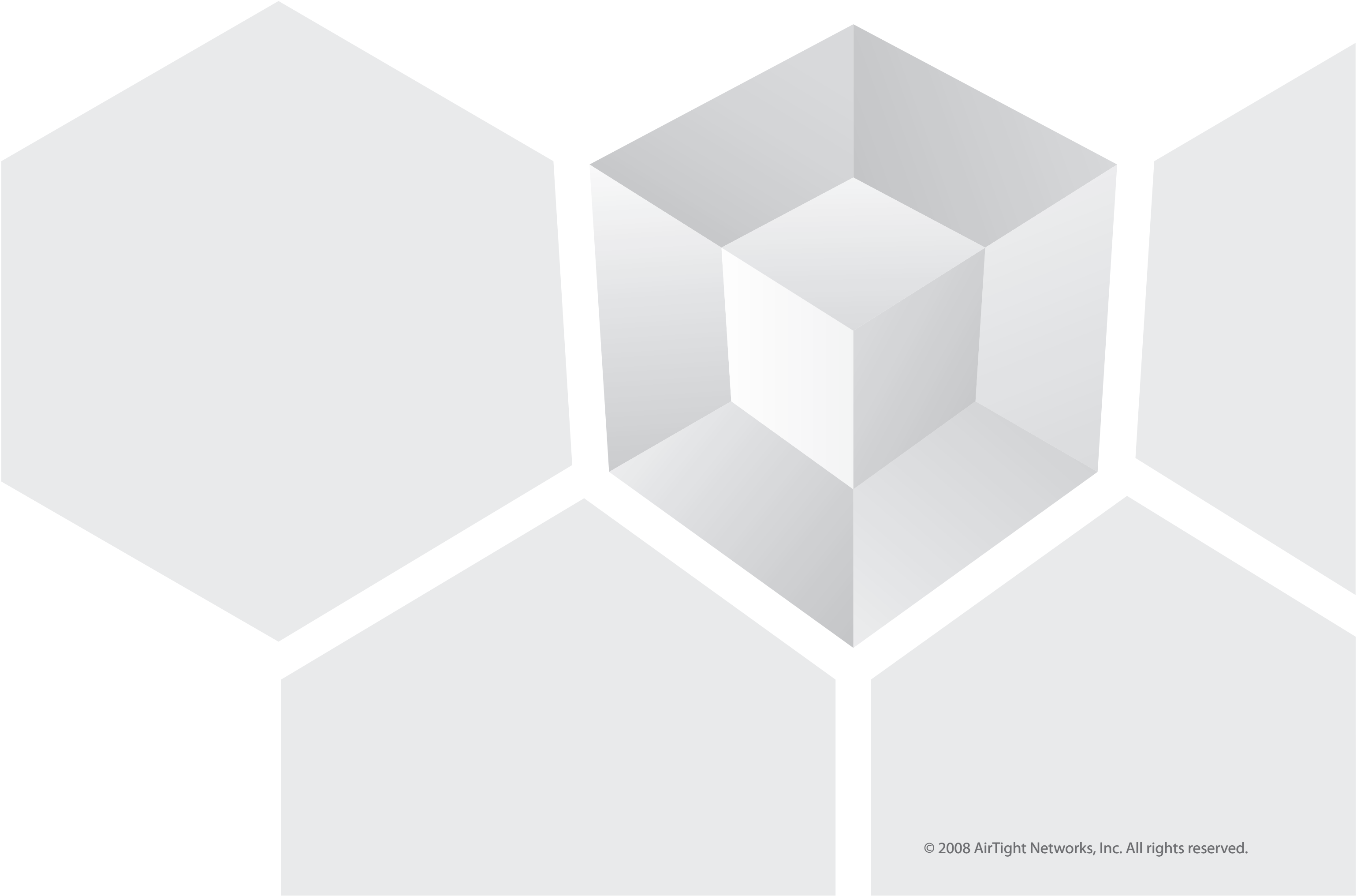
Wireless Vulnerability Management: What It Means for Your Enterprise

A Whitepaper by AirTight Networks, Inc.

339 N. Bernardo Avenue, Suite 200, Mountain View, CA 94043
www.airtightnetworks.com



Executive summary

The instant and obvious benefits of WiFi have made WLANs a big success in public, private, and enterprise sectors. Unfortunately, the adoption of correct security measures for WLANs is lagging far behind the fast pace at which these networks are being deployed. The presence of WiFi in most laptops and handhelds, the simplicity of independently installing WiFi networks, and the ease of exploiting wireless vulnerabilities have together escalated the risks manifold. Even organizations that do not own a WLAN are equally at risk.

A wireless intrusion prevention system (WIPS) is the prevalent approach for mitigating wireless security threats. However, businesses cannot always justify the cost of buying a full-fledged WIPS solution. Some consider the limited WIPS functionality in-built in certain WLAN infrastructure as sufficient. For others that do not own a WLAN, a common misconception is simply having a "no WiFi" policy makes their corporate network immune to wireless threats. A fundamental problem underlying this confusion is that businesses are unable to assess their security posture and fail to comprehend the severity of associated risks. In many cases, they complacently fall back to a "no action" plan leaving them exposed.

This whitepaper revisits the wireless security space, debunks common myths, and presents wireless vulnerability management (WVM) as a proactive strategy to wireless security. WVM is a two-prong approach. Conducting wireless security audits to assess the security posture of a network is the first and necessary step towards managing wireless vulnerabilities. Following, a graded approach can be taken to remediate the vulnerabilities, pass regulatory compliance, and secure critical assets.

Wireless broadband access is becoming a lifestyle. WiFi networks are everywhere: from offices, warehouses, retails stores, and schools to hotel lobbies, airports, coffee shops, and on the street. WiFi is easy to install and convenient to use. The plug-and-play nature of the technology and the unguided nature of the wireless medium that are central to the benefits of WiFi are also the primary reasons that make WLANs inherently vulnerable to a security breach.

The simplicity allows users to buy inexpensive off-the-shelf equipment and install it independently, without bothering about the ramifications of their action. Most users do not comprehend the associated risks. The invisible radio waves used for transmission make the traditional "harden-the-network-perimeter" security approach obsolete. Radio waves often spill beyond the confines of a building. Malicious hackers in the airspace can use these waves to enter your network and steal sensitive data. This means that even a single wireless device on your premises, let alone a wireless LAN, can open a wireless backdoor to your corporate backbone network that is otherwise protected by non-wireless firewalls and intrusion detection systems.

Wireless security is commonly misunderstood as security *for* wireless networks. In fact, wireless security today is an inevitable piece of the overall network and data security puzzle. So, the right question to ask is not 'Is my wireless network secure?' but 'Is my network *wireless-secure?*'.

Escalating Risks from Wireless Vulnerabilities

Businesses are increasingly relying on WiFi, but without appropriate security measures, they are prime candidates for a security breakdown. The recent wireless security survey (published in June 2007) conducted in areas of New York, London, and Paris by RSA, The Security Division of EMC, reported the following:

- **Exponential increase (up to 160%) in the number of WiFi access points (APs) in one year.**
- **Over 20% APs in all three cities were unprotected giving easy access to unauthorized users.**
- **Up to 30% APs had factory-default settings, which grossly violate best practices norms of operating WLANs and are highly vulnerable.**
- **Up to 76% APs were identified as hotspots that provide Internet access in public places; some hotspots are potentially fake (*aka* honeypots) and used for identity theft and stealing sensitive data.**
- **The survey concluded: "Continued education for both businesses and consumers regarding [wireless] security considerations, best practices, and the potential for corporate disruption, is essential."**

Surveys of this nature, commonly termed as "wardriving," can be conducted with standard equipment, e.g., laptop with WiFi. Most wireless vulnerabilities can be exposed and exploited with minimal expertise, using off-the-shelf hardware, and hacking tools freely available on the Internet.

It cannot be stressed more that lapse in wireless security can have drastic repercussions: financial loss, privacy infringement, damage of reputation, thrashing of customer confidence, and litigations and Government regulatory actions. Here are just few examples:

- **In January 2007, TJX Companies disclosed massive security breach (cost projected at one billion dollars over five years by Forrester Research). At least 45.7 million credit- and debit-card numbers and personal information such as social security numbers, driver's license numbers, and military identification of 451,000 customers was stolen. The breach was initiated using the flawed WEP-encrypted WLAN at the Marshalls store near St. Paul, Minnesota in July 2005.** ***[The Wall Street Journal Online, May 4, 2007]***
- **Political consultant Meridian Pacific Inc. was accused of illegally hacking into the South San Joaquin Irrigation District (SSJID)'s wireless network and accessing sensitive documents. Investigators found the SSJID WLAN was unprotected and anyone could enter their network through wireless access without username and password.** ***[Recordnet.com, September 30, 2005]***
- **Hackers, sitting in a parking lot outside Lowe's store in Southfield, Michigan, entered into Lowe's corporate network using an open WLAN. Hackers gained access to servers across 7 US states, planted credit card data sniffing software, and crashed the point of sale system.** ***[Security Focus, November 12, 2003]***
- **GE Money in Finland reported €200,000 stolen in a security breach. GE Money data security manager and accomplices were found guilty of stealing account information and the money; they had used a neighboring unprotected WLAN to covertly enter the private network.** ***[Techworld, August 22, 2005]***

Different Faces of Wireless Vulnerabilities

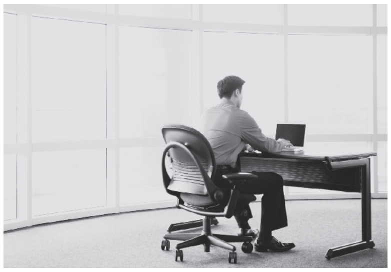
Wireless vulnerabilities come in different shapes and sizes. They can be classified in the following three ways.

Outside-in vs. Inside-out: The spillage of radio waves outside a premise makes the wireless LAN (WLAN) accessible to outsiders. This scenario opens up "outside-in" vulnerabilities—those that can be exploited by unauthorized users to enter your network. Another implication, even for organizations that do not own a WLAN, is that radio waves from an external WLAN can spill into your airspace making wireless access available to employees with WiFi gadgets. This opens up "inside-out" vulnerabilities as employees using such access violate corporate security policies, e.g., firewalls and URL filters.

Employees may use external wireless access for downloading illegitimate content or for transferring sensitive company data over unprotected wireless links. Malicious hackers can advertise fake WLANs to lure users, eventually exploiting wireless as a backdoor to enter a company's private network.

Protocol vs. Implementation: Vulnerabilities can occur as a weakness in the wireless protocol, e.g., limitations of WEP encryption, flaws in the 802.11 (WiFi) standards. Attacks that exploit flaws in the standard are particularly difficult to detect unless the illegitimate device is identified. While the 802.11 standards (e.g., 802.11i and w) are continually evolving for better security, they address only a subset of flaws in legacy protocols. Besides, newer attacks are constantly being discovered putting WLAN security measures at risk of obsolescence. Vulnerabilities also arise from a flaw in the implementation, e.g., software driver of WiFi radio. Poor implementation of AP or client software or ways in which it is managed by the operating system can allow a hacker to crash or disable the device, or take control of the device and use it as a backdoor to enter the wired corporate network to which it is connected.

AP vs. Client: Misconfigured APs and clients (e.g., WiFi laptops) are common targets of security attacks. The recent Café Latte attack is an example of exploiting a misconfigured client using WEP, even when it is not associated with an AP. Attacks such as MAC spoofing and denial-of-service (DoS) can be launched selectively on a client or an AP for potentially disrupting the entire WLAN.



Common Myths about Wireless Security

Understanding of wireless security is unfortunately marred by many myths. Plug-and-play wireless users tend to blindly follow diktats without confirming their veracity, in turn contributing to wireless malpractices galore. Myths about wireless security can be both dangerous and costly—giving a false sense of security to organizations while exposing their private network and data to outsiders. Here, we dispel the common myths about wireless security.

Myth #1: My wireless LAN is safe because I have a firewall securing my wired corporate LAN from the Internet.

Non-wireless security solutions such as firewall and intrusion detection systems operate at layer 3 (i.e., network layer) and above. A wireless LAN presents a potential entry point into your wired corporate LAN at layers 1 and 2 (i.e., physical and link layers), circumventing all wired security measures.

Myth #2: I already got my wired corporate LAN scanned from an auditor, so I do not need to worry about wireless security threats.

Non-wireless scanning tools are powerful in detecting anomalies and vulnerabilities on a wired network. But they fail to capture vulnerabilities at layers 1 and 2 of the wireless LAN. It is a good idea to periodically audit your network against wireless vulnerabilities.

Myth #3: My company does not own a wireless LAN, so I do not need to worry about wireless security threats.

Though an enterprise may not own a wireless LAN, today, it is almost impossible to remain isolated from the wireless presence. Employees using laptops may inadvertently access external WLANs exposing the inside-out wireless vulnerabilities. Employees may deploy a rogue AP or unauthorized, malicious users may connect wireless devices opening backdoors to your organization's private backbone network and sensitive data. Hence, even if an enterprise does not officially deploy a WLAN, it must address the wireless security threat and ensure that a "no WiFi" policy is truly enforced on the premises.

Myth #4: We use WEP to secure all our WiFi communication, so our over-the-air data is secure.

The legacy Wired Equivalent Privacy (WEP) encryption gives a false sense of security. It is well-known that WEP is broken and can be compromised in minutes exposing over-the-air data. Using WEP is widely considered as a malpractice by wireless security experts. Organizations should replace WEP by more recent, stronger alternatives such as WPA2 or at least adopt other remediation solutions that proactively protect WEP devices.

Myth #5: We use WPA\WPA2\802.11i for all our WiFi communication, so our network is secure.

As a response to the flaws in WEP, WiFi Protected Access (WPA) was proposed. It was upgraded to WPA2-the implementation of the IEEE 802.11i standard. WPA or WPA2, if used with pre-shared key (PSK) are still vulnerable to dictionary attacks that can crack the password. Further, simply using WPA/WPA2 does not secure your network. Vulnerabilities such as rogue APs, clients misassociating with external APs and ad-hoc networks that bypass your security policy control can still expose your data and network to unauthorized access. Denial-of-service attacks can also continue to disrupt your WLAN.

Myth #6: LEAP enables effective WLAN security.

The Lightweight Extensible Authentication Protocol (LEAP) is a proprietary security solution developed by Cisco. The authentication mechanism in LEAP, based on the MS-CHAPv2 protocol, is known to be flawed. It can be exploited using a brute force dictionary attack, and has in fact been rated by the CVE standard as a highest severity vulnerability.

Myth #7: MAC address filtering on wireless access points is effective in securing WLANs.

Bypassing MAC filtering is easy. Freely available software tools can be used to sniff MAC addresses being used by devices in the vicinity. MAC spoofing is one of the easiest attacks to launch, and filtering MAC addresses does not provide any security for your wireless LAN. MAC filtering is not only ineffective, but it is cumbersome to maintain for a reasonable-sized wireless LAN.

Myth #8: Turning off SSID broadcast is a step towards securing a WLAN.

It is a common misconception that turning off SSID broadcast on a wireless AP will not allow unauthorized users to discover the AP. Freely available software tools exist that actively probe and discover APs that respond to these probes. Passive sniffing of wireless traffic can also allow hackers to discover wireless APs in the vicinity. Turning off SSID broadcast is not only ineffective, but it in fact leads to another severe vulnerability. Authorized clients that usually connect to enterprise APs, probe for the hidden SSID. A hacker can sniff this information and use it to launch a honeypot attack.

Myth #9: Need for wireless security ends in my airspace.

Managing wireless vulnerabilities is not limited to an organization's premises. Wireless users carry their corporate laptops when they travel. If they connect to WLANs outside the premise, say in a coffee shop across the world, they are still at risk. Recent survey by AirTight Networks at several airports in the US and worldwide captured the elevated threats to wireless devices from viral SSIDs and ad-hoc networks. To carry wireless security on the road, wireless client security software—that enforces corporate security policies and manages how a wireless client behaves and connects—is essential.

Myth #10: Need for wireless security is hyped.

Non-wireless vulnerability assessment tools fail miserably to capture wireless vulnerabilities and hence tend to mislead users in believing that wireless vulnerabilities do not exist. Businesses can ignore wireless security at their own peril. The RSA survey is only one of the many published studies across industry and academia that show that wireless is everywhere and so are wireless threats. Recently, advisory firms such as Gartner, SANS, and Farpoint Group have repeatedly ranked wireless security as a top ten concern.

Managing Wireless Vulnerabilities

Wireless vulnerability management is a continuous process of appraising a network's wireless threat exposure followed by appropriate remediation. After taking steps to repair and close the holes in the network, the network should be scanned again for vulnerability assessment. This follow-up scan will complete the vulnerability management loop. Comparing the pre- and post-remediation reports will help confirm if the network threat exposure has been indeed reduced to an acceptable level.

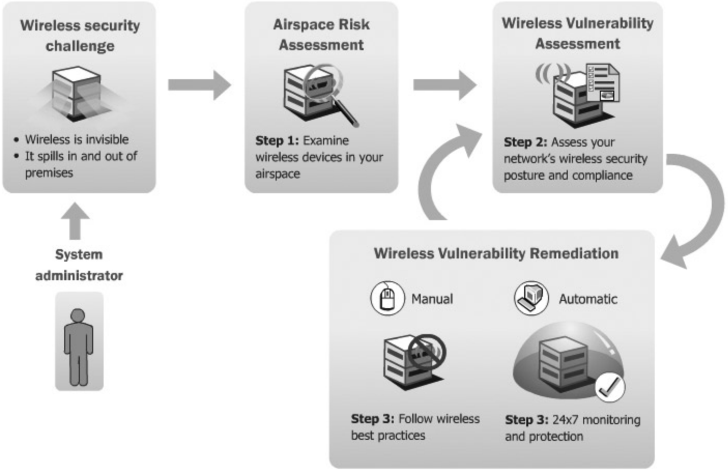

Wireless security challenge
• Wireless is invisible
• It spills in and out of premises
System administrator
Airspace Risk Assessment
Step 1: Examine wireless devices in your airspace
Wireless Vulnerability Assessment
Step 2: Assess your network's wireless security posture and compliance
Wireless Vulnerability Remediation
Manual
Automatic
Step 3: Follow wireless best practices
Step 3: 24x7 monitoring and protection

Figure 1. Wireless Vulnerability Management Lifecycle

Airspace Risk Assessment: Know your environment

Wireless security begins by first gaining visibility into the wireless presence (active wireless devices) in your airspace and assessing the potential risk it poses. The next measure is then to identify your authorized networks (SSIDs) and classify your authorized devices. This classification is a prerequisite to an accurate wireless vulnerability assessment.

Wireless Vulnerability Assessment: Knocking on Your Wireless Backdoor

Wireless intrusion detection and prevention is reactive: attacks are detected and dealt with after they occur. Wireless vulnerability assessment is proactive: instead of waiting for a malicious hacker to break into a network, the network is scanned for vulnerabilities before they can be exploited. In essence, it provides a third-party evaluation or a "hacker's eye view" of a network's exposure to wireless threats.

In addition to protecting their assets, organizations are liable to protecting their consumers' sensitive data, e.g., credit card information in the retail sector, patient data in hospitals, protecting children in schools from getting exposed to illegal content, and personal identity information such as driver's license and social security numbers. Depending on the segment they belong to, organizations are required to comply with legislative regulations such as PCI, SOX, HIPAA, GLBA, and DoD.

An effective wireless vulnerability assessment solution should:

- **Automatically scan for all known vulnerabilities enabling zero-day attack protection**
- **Accurately detect and locate existing and potential vulnerabilities without false positives**
- **Create an inventory of critical assets and unauthorized devices in the airspace**
- **Present the scan results in a concise, but informative report that classifies vulnerabilities, prioritizes them according to well-defined severity levels, summarizes the main findings, and recommends remedial actions**
- **Compare reports generated at different times**
- **Map wireless vulnerabilities in the context of the relevant regulatory compliance**

Wireless Vulnerability Remediation

The logical next step after wireless vulnerability assessment is remediation of detected vulnerabilities. Given the different flavors of vulnerabilities, a one-size-fits-all remediation will not work. Here are different types of remediation methods broadly classified into two categories: Manual and Automatic.

1. **Configuration**
   Wireless vulnerabilities begin with misconfigured devices. The least a network administrator must do is to ensure that operational settings of all authorized wireless devices follow the widely accepted best practices and compliance recommendations.

2. **Software patch**
   When a software bug in a wireless driver is discovered, the vendor usually publishes a software patch to fix the bug. It is critical to keep your wireless software up-to-date. In addition, wireless security vendors may also provide software patches to APs and clients for protecting them against protocol flaws. Using these patches will raise the bar for potential hackers.

3. Wireless client security software

A wireless security software installed on client devices can help organizations enforce wireless security policies on all authorized clients even when they are "on the road." It can also play an important role in the overall wireless security by reporting anomalous activities in its vicinity.

4. Wireless security solution

A wireless security solution provides automatic 24x7 monitoring and protection of wireless airspace. A good solution should:

- **Enforce global wireless security and usage policies, e.g., regulatory compliance, and corporate policies including "no WiFi"**
- **Detect anomalies and attacks**
- **Locate source of anomalous activities**
- **Isolate source of anomalous activities and prevent an attack**

Remediation methods 1 and 2 can be classified as strictly "manual" solutions and methods 3 and 4 can be classified as "automatic" solutions.

About AirTight Networks

AirTight Networks is the global leader in wireless security and compliance solutions providing customers best-of-breed technology to automatically detect, classify, locate and block all current and emerging wireless threats. AirTight offers both the industry's leading wireless intrusion prevention system (WIPS) and the world's first wireless vulnerability management (WMV) security-as-a-service (SaaS). AirTight's award-winning solutions are used by customers globally in the financial, government, retail, manufacturing, transportation, education, healthcare, telecom, and technology industries. AirTight owns the seminal patents for wireless intrusion prevention technology with 11 U.S. patents and two international patents granted (UK and Australia), and more than 25 additional patents pending. AirTight Networks is a privately held company based in Mountain View, CA. For more information please visit www.airtightnetworks.com

AirTight Networks, Inc. 339 N. Bernardo Avenue #200, Mountain View, CA 94043
T +1.877.424.7844 T 650.961.1111 F 650.961.1169 www.airtightnetworks.com info@airtightnetworks.com

AirTight® NETWORKS