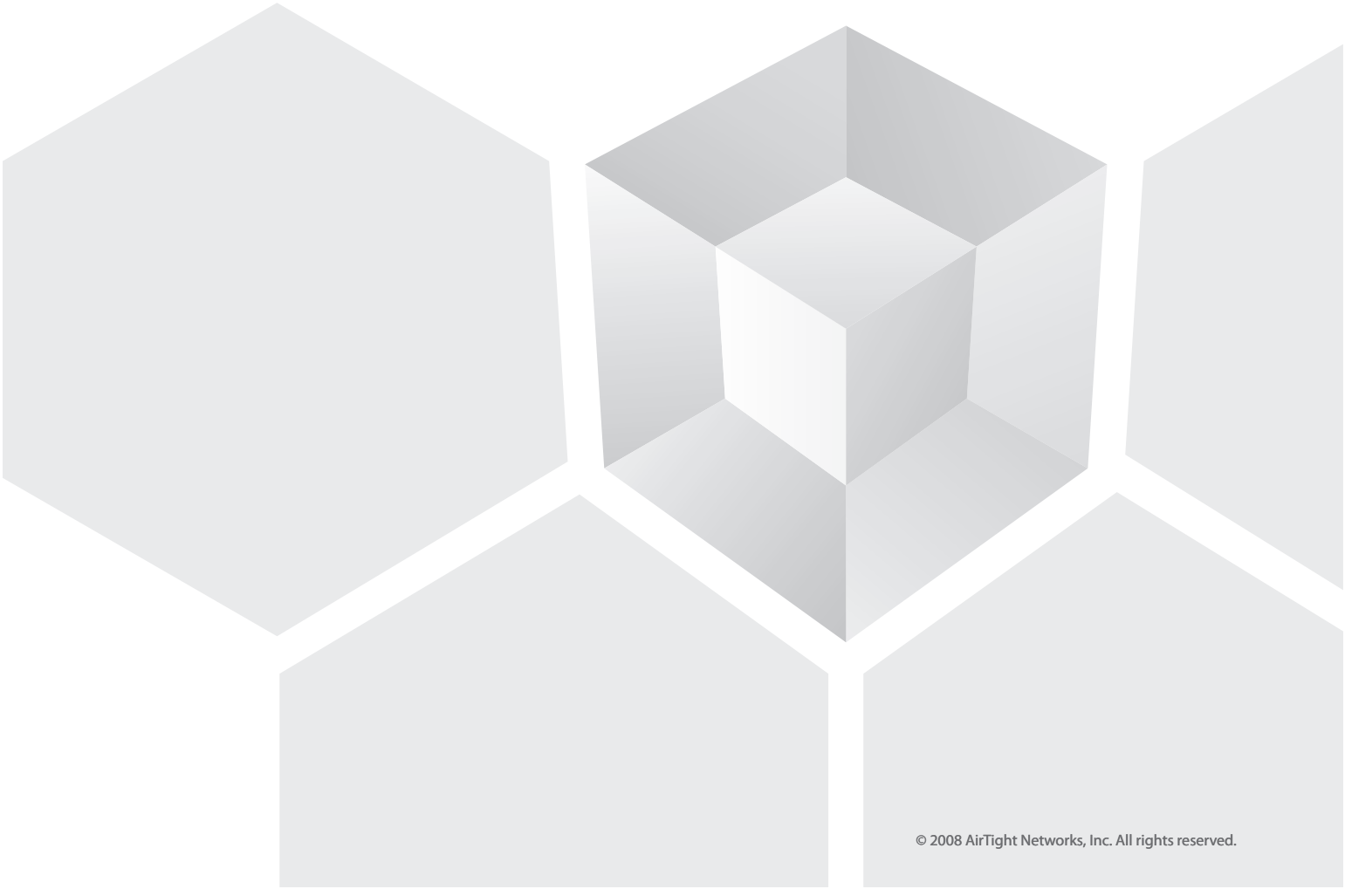
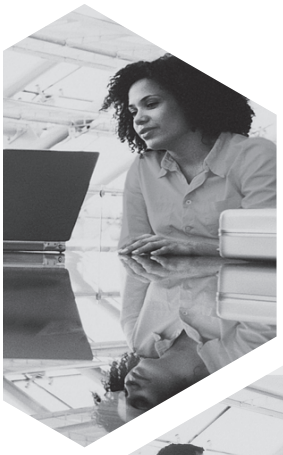
Dispelling Top Ten Wireless Security Myths

A Whitepaper by AirTight Networks, Inc.

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



Dispelling Top Ten Wireless Security Myths



Understanding of wireless security is unfortunately marred by many myths. Some are even propagated as wireless LAN best practices. Plug-and-play wireless users tend to blindly follow these diktats without confirming their veracity. In turn, they only end up contributing to wireless malpractices galore. Myths about wireless security can be both dangerous and costly. Many organizations spend valuable resources in implementing these urban legends that give a false sense of security and leave private networks and sensitive data exposed.

In this paper, we will revisit and debunk top ten wireless security myths.

Myth #1: My wireless LAN (WLAN) 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 WLAN 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. Your authorized users can bypass your firewall policies and content filters using wireless access and connect to potentially dangerous external WLANs. In short, wireless has made the traditional "harden-the-network-perimeter" approach obsolete.

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 using appropriate wireless vulnerability assessment solutions.

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

Even if an enterprise does not own a wireless LAN, today, it is almost impossible to remain untouched by the wireless presence. Employees may deploy a rogue AP or unauthorized, malicious users may connect wireless devices opening backdoors to your organization's private backbone network. Employees using laptops may access external WLANs exposing 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. Hence, even if an enterprise does not officially deploy a WLAN, it must address the wireless security threat.

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.

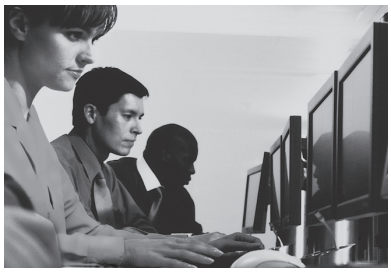
The Lightweight Extensible Authentication Protocol (LEAP) is a proprietary security solution developed by Cisco. The authentication mechanism in LEAP, based on the MS-CHAPv2 protocol, is known to be flawed. It can be exploited using a brute force dictionary attack, and has in fact been rated by the CVE standard as a highest severity vulnerability. Even using strong passwords with LEAP does not obviate the threat.

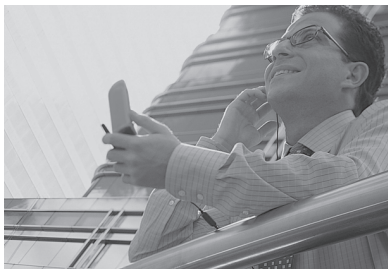
Myth #7: MAC address filtering on wireless access points is effective in securing WLANs.

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. Many published studies across industry and academia show that wireless is everywhere and so are wireless threats. Recently, advisory firms such as RSA, Gartner, SANS, and Farpoint Group have repeatedly ranked wireless security as a top ten concern.

To conclude, stay away from these fallacies. Implement real security measures for protecting your networks and data.

Dispelling Top Ten Wireless Security Myths

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

Wireless Vulnerability Management

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