WHITE PAPER

Wireless LAN Security: What Hackers Know That You Don't

Wireless LAN Security: What Hackers Know That You Don't

This white paper describes the methods, skills, and tools that hackers use to exploit vulnerabilities in 802.11 wireless LANs. A good understanding of hacker tools and techniques and the vulnerabilities they exploit enables security managers to take pro-active steps to properly secure their wireless networks and mitigate security risks.

1. The Challenge of Wireless LAN Security

Because of their flexibility, affordability, and ease of installation, the use of wireless local area networks (wireless LANS, WLANs, and Wi-Fi) are increasing at a tremendous rate. According to In-Stat MDR estimates, there are currently more than 75 million wireless LANs in use worldwide, with 40 million more estimated to begin operation this year. META Group and In-Stat/MDR estimate that 95% of corporate laptop computers that will be shipped in 2005 will be equipped for wireless operation. An equal amount of wireless support devices, such as access points, routers, printers, scanners, and handhelds, are also being produced to meet the demand for wireless.

As wireless LAN deployments increase, so does the challenge to provide these networks with security. Wireless LANs face the same security challenges as their wired counterparts, and more. Because the medium for wireless is air, wireless LANs have the added issue of securing data that travels the airwaves. This has given momentum to a new generation of hackers who specialize in inventing and deploying innovative methods of hijacking wireless communications.

Some enterprises believe they do not have to concern themselves with wireless security if they run non-mission-critical systems with non-sensitive information on their wireless LANs. This can be a costly mistake, since most enterprise wireless LANs connect back to a wired network at some point. Hackers can use a user laptop as an entry point into the entire enterprise network!

2. Risks and Vulnerabilities of Wireless LANs

Along with the many conveniences and cost-saving advantages to wireless LANs, there are also some inherent risks and vulnerabilities.

The Nature of the Wireless Medium

Traditional wired networks use cables to transfer information, which are protected by the buildings that enclose them. To access a wired network, a hacker must bypass the physical security of the building or breach the firewall.

On the other hand, wireless networks use the air, which is an uncontrolled medium. Wireless LAN signals can travel through the walls, ceilings, and windows of buildings up to thousands of feet outside of the building walls.

Additionally, since the WLAN medium is airwaves, it is a *shared medium that allows any one in proximity to "sniff" the traffic*. The risks of using a shared medium is increasing with the advent of readily-available "hacker's tools." A variety of specialized tools and tool kits enable hackers to "sniff" data and applications, and to break both the encryption and authentication of wireless data.

Insecure Wireless LAN Devices

Insecure wireless LAN devices, such as access points and user stations, can seriously compromise both the wireless network and the wired network, making them popular targets for hackers.

Insecure Access Points

Access points can be insecure, due to improper configurations and design flaws.

Access points ship with default configurations that are insecure. They are pre-configured with a default password; they broadcast service set identifiers (SSIDs); and they often require no encryption or authentication. If deployed with default settings, they become gateways that hackers use to access both the wireless and the wired network.

"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

"Through year-end 2004, the employee's ability to install unmanaged access points will result in more than 50% of enterprises exposing sensitive information through wireless networks."

Gartner

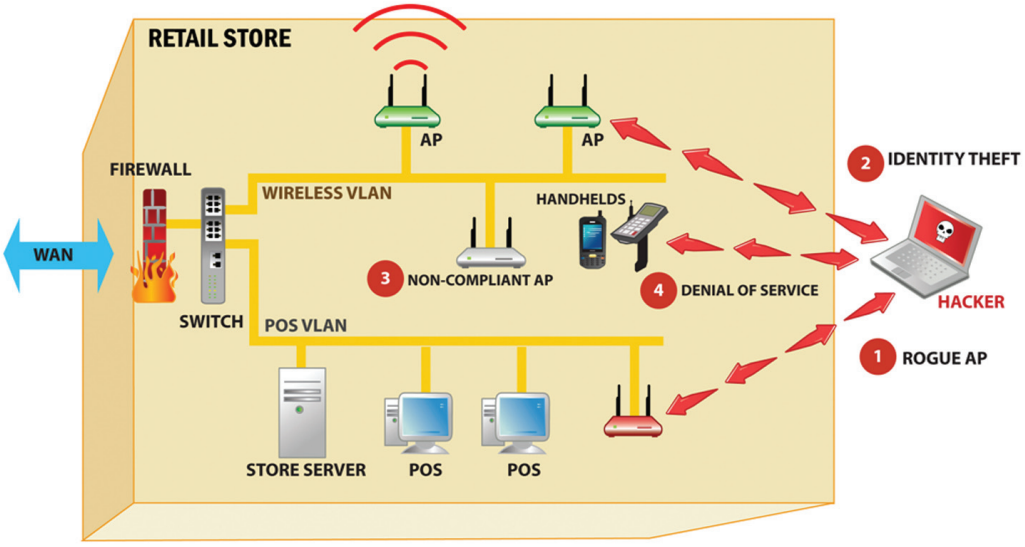

Figure 1: Common Wireless LAN Security Risks

Intruders can convert laptops into "soft" access points (APs) by either using a variety of software programs, such as HostAP, Hotspotter, or Airsnark, or, by simply using a USB wireless adapter. Using soft APs, a hacker can cause a legitimate user to connect to the hacker's own laptop, compromising that user's machine.

Insecure User Stations

Insecure wireless user stations such as laptops or bar code scanners pose even a greater risk to the security of the enterprise network than insecure access points. The default configuration of these devices offer little security and can be easily misconfigured. Intruders can use any insecure wireless station as a launch pad to breach the network

3. Wireless LANs Allow Strangers Easy Access

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 a hacker to connect to a legitimate user's computer, often without their knowledge. This compromises sensitive documents on the user station, and exposes it to even further exploitation. The danger is compounded if the legitimate station is connected to a wired network, which is also now accessible to the hacker.

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

"Unmanaged wireless LANs can jeopardize entire enterprise networks, data, and operations."

Forrester Research, Inc.

4. The Hacker's Toolbox

Wireless LAN hacking tools are widely available for free on the Internet, and new tools are introduced every week. Security managers must familiarize themselves with these tools to learn how to protect themselves. The table below lists some common freeware hacker's tools.

Table 1: Common Freeware Hacking Tools

Tool	Website	Description
NetStumbler	http://www.netstumbler.com	Freeware wireless access point identifier that listens for SSIDs and sends beacons as probes that search for access points
Kismet	http://www.kismetwireless.net	Freeware wireless sniffer and monitor that passively monitors wireless traffic and sorts data to identify SSIDs, MAC addresses, channels, and connection speeds
THC-RUT	http://www.thehackerschoice.com	Freeware wireless LAN discovery tool that uses "brute force" to identify low traffic access points. ("Your first knife on a foreign network.")
Etherea	http://www.ethereal.com	Freeware wireless LAN analyzer that interactively browses captured data, viewing summary and detail information for all observed wireless traffic
AirSnort	http://airsnort.shmoo.com	Freeware encryption breaker that passively monitors transmissions, computing the encryption key when enough packets have been gathered
HostAP	http://hostap.epitest.fi	Toolkit that converts a wireless LAN user station to function as an access point. (Available for wireless LAN cards that are based on Intersil's Prism2/2.5/3 chipset.)
WEPWedgie	http://sourceforge.net/projects/wepwedgie/	Toolkit for determining 802.11 WEP keystreams and injecting traffic with known keystreams. The toolkit also includes logic for firewall rule mapping, pingscanning, and portscanning via the injection channel
WEPCrack	http://sourceforge.net/projects/wepcrack/	Freeware encryption breaker that cracks 802.11 WEP encryption keys using the latest discovered weakness of RC4 key scheduling
AirSnarf	http://airsnarf.shmoo.com/	Soft AP setup utility that is designed to steal usernames and passwords from public wireless hotspots by confusing users with DNS and HTTP redirects from a competing AP
SMAC	http://www.klcconsulting.net/smac	Windows MAC Address Modifying Utility that allows users to change MAC address Network Interface Cards (NICs) on Windows 2000, XP, and 2003 Server systems, regardless of whether or not the manufacturer allows this option
Airjack	http://sourceforge.net/projects/airjack/	Denial-of-Service tool kit that sends spoofed authentication frames to an AP with inappropriate authentication algorithm and status codes. AP then drops connections with stations. Includes WLAN_JACK, Monkey_JACK, and hunter_killer
IRPAS	http://www.phenoelit.de/irpas/	Internet Routing Protocol Attack Suite designed to attack common routing protocols including CDP, DHCP, IGRP and HSRP

"Wireless LANs are too easy to install and manipulate, and users and criminals will continue to take advantage of opportunities to disrupt or damage enterprise networks."

Gartner

Table 1: Common Freeware Hacking Tools (continued)

Tool	Website	Description
Ettercap	http://ettercap.sourceforge.net	Suite for Man-in-the-Middle attacks. It features sniffing of live connections and content filtering on the fly. Additionally, it supports active and passive dissection of many protocols and includes many features for network and host analysis
Cain&Abel	http://www.oxid.it	Password recovery tool that allows easy recovery of various kinds of passwords by sniffing the network and cracking encrypted passwords using Dictionary, Brute-Force, and Cryptanalysis attacks. Decodes scrambled passwords and analyzes routing protocols
Hotspotter	www.remote-exploit.org/codes.html	Passively monitors the network for probe request frames to identify the preferred networks of clients. Acts as an access point to allow the client to authenticate and associate
WEP Attack	http://sourceforge.net/projects/wepattack/	Brute-Force WEP cracker that uses Dictionary attacks against WEP keys. Is usually very effective against residential gateways
ASLEAP	http://asleap.sourceforge.net/	Toolkit that can recovers weak LEAP passwords, read captured files, or sniff the air. Can also actively de-authenticate users on LEAP networks, forcing them to re-authenticate
THC-LeapCracker	http://www.thc.org	Toolkit that can break the Cisco LEAP authentication protocol and can also spoof challenge-packets from access points, allowing the hacker to perform Dictionary attacks against all users
DSNIFF	http://naughty.monkey.org/~dugsong/dsniff	Collection of tools for network auditing and penetration testing. Can passively spy and perform Man-in-the-Middle attacks
IKEcrack	http://ikecrack.sourceforge.net/	Authentication crack tool that can use Brute-Force or a Dictionary attack against key/password used with Pre-Shared-Key IKE authentication
Nessus	http://www.nessus.org	Remote security scanner

Wireless LAN Scanner & Sniffer Tools

User-friendly Windows-based freeware tools such as NetStumbler probe the airwaves searching for access points that broadcast their SSIDs, providing easy ways for hackers to find open networks. More advanced tools, such as Kismet, have been introduced on the Linux platform. Kismet passively monitors and captures wireless traffic.

Both NetStumbler and Kismet use global positioning system (GPS) information to map the exact locations of wireless LANs. "War drivers" and intruders use these tools to locate the physical presence of wireless LANs, regardless of whether they are secure or unsecured. War drivers drive around cities searching for wireless LAN signals. This information is then posted on websites such as www.wigle.net (which lists more than 700,000 access points and 1,100,000 wireless networks) and www.wifinder.com. Hackers use these listings to look for access points with the same SSID, access point MAC addresses, or the physical number of access points in a given address or location.

Antennas

To connect with wireless LANs over a distance, hackers either use long-range, commercially available antennas, or build their own from Pringle® cans or any similar metal cylinder. These antennas enable hackers to receive 802.11 signals from several thousand feet away. They can access the network while remaining completely out of sight..

Tools That Break WEP Encryption

Hackers use tools such as WEPwedgie, WEPCrack, WEPAttack, BSD-Airtools, and AirSnort to break the Wired Equivalent Privacy (WEP) encryption standard. These tools exploit vulnerabilities in the WEP encryption algorithm by passively observing wireless LAN traffic until they collect enough data to recognize the pattern. They then use this information to break the encryption key. WEPwedgie and BSD-Airtools 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.

Typically, in a manual WEP set up, most deployments use a single key out of four, allowing a much easier time to completely compromise the network. Though vulnerable, WEP is still in use today. The next generation of encryption uses Temporal Key Integrity Protocol (TKIP, pronounced tee-kip) to provide per-packet key mixing, an integrity check, and a re-keying mechanism. The keys are changed often enough to prevent compromise, but since the data is sent over the air, it can be captured. If not encrypted, the data can then be decoded.

Tools That Break Authentication

Hackers use tools such as THC-LEAPCracker to break or compromise variations of the widely-used, port-based authentication protocols for 802.1x wireless, such as Lightweight Extensible Authentication Protocol (LEAP) and Protected Extensible Authentication Protocol (PEAP).

These protocols were designed for use by wired networks, which reside in a physically secure environment. When deployed in the shared and uncontrolled wireless environment, it becomes easy for hackers to spoof, jump in the middle, or sniff authentication credentials.

The Institute of Electrical and Electronics Engineers, Inc. (IEEE) is currently working on new standards, including 802.11i, which are expected to be ratified in late 2004 or early 2005.

5. Common wireless LAN Attacks

This section describes some common attacks on wireless LANs that represent significant risks. With the variety of hacker's tools widely available on the Internet, a novice hacker can perform a multitude of published, cookbook attacks.

Malicious or Accidental Association

A hacker can force an unsuspecting user station to connect to an undesired/spoofed 802.11 network, or alter the configuration of the station to operate in an ad-hoc networking mode. To begin, the hacker sets up a laptop as a soft access point using either freeware hacker's tools, such as HostAP, AirSnarf, or

"As wireless networks become ubiquitous extensions of wired networks, problems with rogue access points will wane — though accidental network associations and attacks against mobile laptops will increase. This makes it very important to understand the risks of wireless LAN laptops and other devices that are present in every organization."

Gartner

"Once a hacker is associated with a LAN, the hacker is in that LAN and difficult to detect."
Gartner

Hotspotter, or a commercially available tool. (Companies such as PCTel provide commercial software that converts 802.11 devices into access points.)

As the victim's user station broadcasts a request to associate with an access point, the hacker's soft access point responds to this request and establishes a connection between the two. Next, the soft access point provides an IP address to the victim's user station. Once this is done, the hacker can scan the victim's station with tools designed to find Windows' vulnerabilities. The hacker can then steal information, install Trojan horses or other spyware, and if it is connected to the wired network, use the victim's station as a launch pad to get access to other servers.

Wireless LANs are subject to diversion. Stations do not always know to which access point or network they are connecting. Stations can be tricked or forced to connect to a malicious access point, since there is often no authentication of the access point. This is Open System Interconnection (OSI) Layer 2 (data link) vulnerability. Layer 3 (network) authentication offers no protection against it, nor does the use of virtual private networks (VPNs). Wireless LANs with 802.1x-based authentications (at Layer 2) do help protect against malicious associations, but are vulnerable.

A malicious associations attack does not try to break the VPN or other security measures. Instead, it takes over the client at Layer 2.

To prevent user stations from connecting to unauthorized access points and networks, enterprises must constantly monitor the airwaves of their wireless LANs to be aware of any potential hazards.

Identity Theft (MAC Spoofing)

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 (PINs) 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.

Some enterprises secure their wireless LAN by using an authorized list of station MAC addresses for authentication. While this method provides some security for smaller deployments, MAC addresses were never intended for this use.

Even if you are using encryption or VPN, MAC addresses are always in the air. With software tools such as Kismet or Ethereal®, a hacker can easily capture the MAC address of a valid user. To perform identity theft, a hacker can change his MAC address to the victim's MAC address using a spoofing utility such as SMAC (Spoof MAC), or, manually change the Windows registry entry. Once this has been done, the hacker can connect to the wireless LAN, bypassing any MAC address filtering.

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 tools like ASLEAP and THC-LeapCracker. Other authentication schemes, such as EAP-TLS and PEAP, may require more sophisticated attacks that exploit other known vulnerabilities in wired side authentication schemes, but are feasible.

RF monitoring allows users to ensure that proper authentication is being enforced. In addition, excessive authentication attempts may also indicate a malicious attempt by a hacker.

Man-in-the-Middle Attacks

One of the more sophisticated attacks, the Man-in-the-Middle attack, breaks VPN connections between authorized stations and access points by inserting a malicious station between the victim's station and the access point. The hacker becomes the "man in the middle."

These attacks are very similar to wired side Man-in-the-Middle attacks, and tools to exploit these attacks on the wired-side can be easily used on the wireless network. Getting into the middle of a communication session is a problem on the wired side. This process is much easier with wireless networks. Using SoftAP software, a hacker can easily convert a wireless device into a soft access point, and position that access point in the middle of the communication session.

The more sophisticated Man-in-the-Middle attack preys upon challenge and handshake protocols to perform a de-authentication attack. The de-authentication attack knocks a user from an access point, causing the user to search for a new access point with which to connect. With the hacker's SoftAP access point running, the user reconnects to the hacker's laptop, PDA, or other device.

Now the hacker, with a different wireless interface, connects to the real wireless LAN, passing all authentication traffic to the real wireless network. The victim is oblivious to this, and passes all data through the hacker. This scenario is possible because VPNs establish their connection at Layer 3 in the OSI model, while wireless exists below the VPN, at Layer 1 and Layer 2.

Once connected, the hacker can use tools like DSNIFF, Ettercap, IKEcrack, or other Man-in-the-Middle tools to downgrade or rollback VPN security until traffic is in either in clear-text, or begins using an easily-broken weak encryption. This is a common problem in most VPN protocols, such as IPSEC, PPTP, SSH, SSL, and L2TP.

Additionally, freeware tools, including Wireless LANjack and AirJack, enable hackers to launch a Man-in-the-Middle attack by automating the multiple steps required to perform it.

Only a highly capable Intrusion Detection System (IDS) and 24-hour monitoring can detect these types of attacks on a wireless LAN. An effective security solution keeps a constant watch on the network, while simultaneously analyzing the network activity. Since this type of attack is not based on a single signature, a wireless IDS must be able to correlate and analyze data to show that this type of attack is occurring.

Denial of Service Attacks

Every network and security manager fears the downtime and loss of productivity that results from a crippling denial of service (DoS) attack. For a wireless network, the attack can come from any direction.

There are several readily-available freeware tools such as Wireless LANJack and hunter_killer that can launch DoS attacks. DoS attacks can be directed against a specific user station to prevent that station from communicating with the network, against a specific access point to prevent stations from connecting with it, or as an attack against all network devices. In this last case, the attack shuts down all wireless LAN activity.

A hacker can abuse the Extensible Authentication Protocol (EAP) to launch a DoS attacks against the authentication server, flooding it with requests to be processed. This prevents valid users from authenticating to the wireless LAN, and causes a DoS across the entire enterprise. Additionally, this can result in an outage of the wired network. "The Unofficial 802.11 Security Web Page" at www.drizzle.com lists forms of DoS attacks launched by manipulating EAP-to-target wireless stations and access points with log-off commands, start commands, premature successful connection messages, failure messages, and other modifications of EAP.

Network Injection Attacks

A newly-developed DoS, the network injection attack, exploits improperly configured wireless LANs or rogue access points to target the entire network. When an access point is attached to an unfiltered part of the enterprise network, it broadcasts network traffic, such as "Spanning Tree" (802.1D), OSPF, RIP, HSRP and other broadcast or multicast traffic. By doing this, the packets invite attacks that take down wireless and wired network equipment and spur a meltdown of the entire internal network infrastructure, including hubs, routers, and switches.

The Spanning Tree algorithm normally ensures a loop-free Ethernet topology for networks that contain parallel bridges and multiple Ethernet segments.

Loops occur when there are alternate routes between hosts. If a loop exists in an extended network, bridges may forward traffic to false or wrong Ethernet hosts indefinitely, increasing traffic and declining network performance to the point where the network stops responding. A hacker can inject traffic onto the wireless LAN segment and it will be propagated through the entire enterprise. This creates a DoS attack by intentionally inserting loops into the network.

Rogue sniffers initiate the DoS attack by echoing manipulated Spanning Tree sessions back to the wireless LAN access point. The access point echoes the packets to other internal hosts, causing a domino effect. Spanning Tree attacks usually render intelligent hubs, bridges, routers, and switches inoperative, requiring the devices to be rebooted or reconfigured to make them functional.

Routing attacks are another popular prey for enterprise DoS attacks. A hacker can use tools such as IRPAS or Routing Attack Tool to inject bogus routing updates into the network, changing the default gateways or destroying routing tables. Any rogue access point on the network that is not filtered by a gateway opens the network to this damaging attack. Motorola has discovered that nearly one out of five corporate networks surveyed are vulnerable to this form of attack.

6. Anatomy of a Simple Wireless LAN Attack

Using a number of simple freeware tools, a hacker can compromise a network by following a few steps. The steps below list the steps a hacker can take to perform a simple wireless LAN attack. These attacks are completely passive in most cases, so impossible to detect, but the longer the hacker is allowed to sniff, the more the data is compromised.

1) Obtain a wireless LAN card that accepts an external antenna. This allows the hacker to receive signals at distances away from their targets. These types of wireless LAN cards can be found on eBay® or companies like Hyperlink Technologies.

2) Become anonymous by using Microsoft's built in firewall software or products like Zone Labs' ZoneAlarm® to protect the computer from "counter-scanning" by IDS systems.

3) Use NetStumbler, a built in wireless client, or another wireless scanner to find open access points, DHCP servers, and IP addresses.

4) Exploit discovered vulnerabilities in the wireless LAN. These methods are the same as those a hacker would use to exploit a wired network. These attacks are completely passive in most cases, so impossible to detect, but the longer the hacker is allowed to sniff, the more the data is compromised.

- Use Ethereal or another protocol analyzer to sniff the airwaves, grab all wireless traffic, and obtain a valid MAC address and IP address.

- Capture wired broadcast traffic (IPX, NetBIOS, ARP, OSPF, Windows Broadcasts, and other types of Traffic) to map out the network.

- Again use Ethereal to look for clear-text protocols, such as Telnet, POP, or HTTP, or to look for authenticated traffic, to capture usernames and passwords.

5) Use tools like SMAC to spoof a MAC address, to bypass any MAC address filters, and eliminate a common known MAC address tied to the user.

6) Use Windows Wireless to add the network to the preferred connection lists, or a client utility to connect to the target wireless LAN

7) Launch a DOS prompt and run IPCONFIG to see if there is an assigned IP address.

8) Roam the network after obtaining an IP address.

9) Use a vulnerability scanner, such as Nessus to scan for vulnerable user stations, and access points, or other devices that are attached to the wireless network.

From the above, it is easy to see that it does not take much expertise to find open access points or user laptops which function as backdoors to log into a corporate network. For this reason, it is important to monitor for any insecure access points or LANs and lock them down.

7. How to Defend against these Threats

As businesses and consumers continue their rapid adoption of wireless technologies, all enterprises must address the growing security concerns from new airborne threats. Companies spend millions of dollars securing their wired networks. When a company's network is left exposed by insecure devices, hackers can enter the organization and compromise the company's corporate backbone, rendering investments in information technology security obsolete. The implications from a security breach can impact the company's reputation, intellectual property and regulated information. The only 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:

1. Locking down the wireless LAN's perimeter (both access points & wireless-enabled stations)

2. Securing communication across the wireless LAN (authentication, encryption & VPNs)

3. 24x 7 Real-time Monitoring of Network Traffic
   Perimeter control for the wireless LAN starts with deploying personal firewalls on every laptop and deployment of enterprise-class access points that offer advanced security and management capabilities. All access points should be completely locked down and reconfigured from their default settings. The SSIDs passwords of the access points should be changed from their default names.

Organizations should deploy strong encryption and authentication standards (for e.g.: WEP, PEAP, WPA, LEAP etc.) and install VPNs to secure communication across the wireless networks.

Like a video camera that monitors all activity in a secure building 24 hours a day, a critical layer of wireless LAN security requires continuous monitoring of the network to identify rogue WLANs, detect intruders and impending threats, terminate and locate unauthorized connections and enforce WLAN security policies. **Motorola's Wireless IPS** provides the most advanced solution for control of the airwaves, security, policy and operational support for wireless networks. As a key layer of security, Motorola's Wireless IPS complements wireless VPNs, encryption & authentication. Using patent-pending technology to correlate and analyze the monitored data, Motorola's Wireless IPS provides the industry's most accurate intrusion prevention for wireless networks.

motorola.com