AIRMAGNET

AN AIRMAGNET TECHNICAL WHITE PAPER

Wireless Security in the Government Environment

by Wade Williamson

WWW.AIRMAGNET.COM

Table of Contents

Introduction

> *Perhaps the most significant difference from wired networks and the main source of these risks is that with wireless networks the organization's underlying communications medium, the airwave, is openly exposed to intruders, making it the logical equivalent of placing an Ethernet port in the parking lot.*
> — National Institute of Standards and Technology[1] (NIST)

Security is at the top of the list of critical missions in government operations from the Department of Homeland Security to any local city government. The leaps in communications and networking technology have enabled new ways of working and mobile applications that were previously unimaginable. Chief among these is wireless networking technology, which by its nature also opened the door to increased risks in security.

The advantages of wireless networking are huge. WLAN has changed the face of modern warfare, enabling soldiers on the ground to communicate with other units and see what the enemy is doing around them. WLAN has enabled an information-rich environment in government and schools though portable computers and handheld devices. The ability to call up information and communicate at any time, in any place, is so valuable that the advantages of WLAN far outweigh its risks. Wireless is here to stay.

But the security risks are real and cannot be downplayed. A technical survey of 802.11 wireless networks from West Point maintains that "By most estimates a significant portion of these networks have no security mechanisms whatsoever."[2]

[1] "Wireless Network Security: 802.11, Bluetooth and Handheld Devices, Recommendations of the National Institute of Standards and Technology" Karygiannis, Tom and Owens, Les, NIST Special Publication 800-48, U.S. Dept. of Commerce, Gaithersburg, MD
[2] "A Survey of 802.11a Wireless Security Threats and Security Mechanisms: A Technical Report to the Army G6," Welch, Colonel Donald J. and Lathrop, Major Scott D., Information

Wireless network administrators in government face a critical challenge in assuring that WLANs under their management are secure from both internal and external intrusion. Fortunately, it is a challenge that can be met through a combination of policy, monitoring and technology.

WLAN Vulnerabilities

Instituting an effective security program begins with understanding existing security measures and their effectiveness and vulnerabilities.

Encryption

You can't prevent hackers from detecting your WLAN's RF signal. The use of directional antennas can help to control the shape of the signal, but they don't completely solve the problem. You can't prevent detection of your signal, but you can do something to make the contents unreadable by unauthorized "listeners." This makes encryption the first, barebones line of defense. It comes built into your WLAN software. When network traffic is encrypted, it may deter the casual or less-adept intruder who is just looking for an easy target. But relying on encryption alone is risky. The initial standard encryption for wireless networking, Wired Equivalent Privacy (WEP) was hacked within weeks of its release.[3]

The next attempt at standard encryption, IEEE's Wi-Fi Protected Access (WPA) bridged the gap until IEEE's recent ratification of an improved 802.11i standard, WPA2. WPA2 employs a different encryption standard, Advanced Encryption Standard (AES). AES has been adopted by NIST and the U.S. Department of

Technology and Operations Center, Dept. of Electrical Engineering and Computer Science, United States military Academy, West Point, NY

[3] *RCR Wireless News*, August 2, 2004, v23 i31 p8

Commerce as the FIPS (Federal Information Processing Standard)140-S specifications for wireless security.[4]

However, enterprises with existing LANs may have to purchase new hardware to support AES.[5] Government organizations should check to assure all WLAN vendors are certified FIPS 140-2 compliant.

IPSec (Internet Protocol Security) and SSL (Secured Socket Layer) are both encryptions used to create VPNs. VPNs are often used to send data over the Internet in a secure “tunnel” that cannot be read or reproduced by unauthorized users. Web-based SSL uses the public-and-private key encryption system from RSA, which also includes the use of a digital certificate. As any Web-enabled machine can be used to access a SSL based VPN, two-way authentication is not available. Anyone with the correct username and password can access the SSL VPN from any PC connected to the Internet.

IPSec works at Layer 3 and secures everything in the network. Unlike SSL, which is typically built into the Web browser, IPSec requires a client installation. IPSec facilitates two-way authentication using DES, a powerful block cipher that is highly resistant to attack because it requires an impractical expenditure of time and resources.

Of course, if the VPN is unsecured at either the network where it begins or the network where it ends, a hacker can waltz right through.

It is the nature of hackers to work long and hard to break encryptions, so it is only a matter of time before someone successfully hacks AES and its successors.

[4] “Wireless Network Security: 802.11, Bluetooth and Handheld Devices, Recommendations of the National Institute of Standards and Technology” Karygiannis, Tom and Owens, Les, NIST Special Publication 800-48, U.S. Dept. of Commerce, Gaithersburg, MD

[5] *RCR Wireless News,* August 2, 2004, v23 i31 p8

Encryption, while necessary, should be viewed as only beginning the task of securing the WLAN.

Device Settings

All devices that form the WLAN — Access Points (APs), mobile computers, handheld devices — come from the factory with the capability of being securely configured. However, they usually arrive in the box with the security settings turned off, or set with default passwords and access channels. Every device attached to the WLAN must be properly configured with passwords and authentication protocols to protect the network.

Rogue Devices

Rogue devices are often introduced into the WLAN by employees who are unhappy with their network performance, and either don't know or don't care about the security risks. Anyone can buy an off-the-shelf AP and set it up near their workstation to improve network throughput.

Rogue APs are a wide-open door to hackers looking for WLAN access. The rogues are not configured for security in most cases, and they are easily detectable by anyone sitting in the parking lot looking for a device with which to associate and penetrate the network.

Another type of rogue AP is when a neighboring WLAN's AP inadvertently associates with your network. While it may be inadvertent, a hacker associating with your neighbor's rogue device can get into your network through the neighbor's WLAN.

Internal Attacks

It has been estimated that internal users create up to a third of the vulnerabilities of the enterprise WLAN. There is the occasional bad apple that steals information or money from his or her employer, but the majority of internal users are not trying to harm the organization; they are just ignorant of the consequences of their actions or failure to take precautions.

As discussed above, there's the person who goes out and buys a cheap AP and sets it up so he (or she) can always run at peak performance and doesn't have to share bandwidth with others in his area. Employees may telecommute from home using wireless technology, or they may take a laptop to a public "hotspot" like an Internet café to check email or catch up on work. Employees need the right MAC address and password to access the enterprise WLAN. However, if the employee's home computer or laptop is using the factory-set default security or no security, that device becomes a "soft AP," broadcasting the MAC address and password freely to any war driver in the street, or the sniffer sipping a latte at the next table.

The SSID (Service Set IDentifier) is the unique name of a WLAN. "War drivers" in cars scan for SSIDs from streets and parking lots. When they find one, they attempt to configure their device to look like a legitimate user of that network. If the network administrator has been careless about encryption, the rogue user can access the network. In newer wireless networks, some administrators disable the automatic SSID to prevent hackers from obtaining it. (Though this is a deterrent only to inexperienced or casual hackers.)

In an effort to combat rogue users, some network administrators have set up Virtual Private Networks (VPNs). Using advanced encryption techniques and the public telephone infrastructure, VPNs create an invisible data tunnel from one WLAN locale to another (say, between an agency's WLAN in Washington, D.C. and its California office), or between one Intranet and another. VPNs are highly secure. However, if one of the WLANs that it connects is `not` secured, the entire system is vulnerable to any hacker that associates with the unsecured network.

External Attacks

No one in government who has worked with networks these past several years doubts the ever-present threat of malicious hackers bent on obtaining access to sensitive information within government WLANs. The tools required to hack networks (like NetStumbler, Kismet, AirSnort and WEPCrack) are available anywhere in the world — for free.

A recent survey by KPMG found that 12% of hackers attempted malicious activities[6], e.g. Denial of Service (DoS) attacks, destruction of data, espionage, theft of financial information or identity theft. The seventh annual Computer Crime and Security Survey undertaken by the FBI and the Computer Security Institute of San Francisco (CSI) found that out of 503 U.S. computer security professionals polled, 90% reported network security breaches within the last 12 months of the survey, while 80% admitted to financial losses due to security breaches. The 44% of respondents who quantified financial losses reported a total of $445,848,000 lost.[7]

Happily, the eighth annual survey by CSI and the FBI shows that financial damages from attacks on networks have dropped for the fourth straight year in a row. The survey reported that one of the reasons was an increasing percentage of respondents (73%) have implemented intrusion detection/prevention technology. The previous year, only 60% reported implementing intrusion detection/prevention technology. [8]

[6] *Computer Weekly*, Feb. 10 2004 p30
[7] *National Underwriter Life & Health-Financial Services Edition*, June 17, 2002, v106 i24 p30.
[8] *Government Computer News*, Sept. 29, 2003, v22 i29 p32.

How Hackers Attack The Wireless Network

Being an innovative group, hackers are continually coming up with new ways to penetrate network defenses. But their attacks can generally be grouped into these categories:

- MAC spoofing
- Denial of Service
- Malicious association
- Man-in-the-middle attacks

MAC Spoofing: Hackers use MAC spoofing to impersonate a legitimate network user. All network interface cards (NICs), like PCMCIA or PCI cards, provide a mechanism for changing their MAC addresses, issued by the manufacturer, that identify a specific device. In many cases, the MAC address is used as an authentication factor in granting the device access to the network, or to a level of system privilege to a user.

The hacker will change his device's MAC address to that of a user and thus gain access to the network. If the hacker is using the MAC address of a top executive with access privileges to sensitive material, a great deal of damage can be done.

Attackers employ several different methods to obtain authorized MAC addresses from the network. A brute force attack uses software that will try a string of random numbers until one is recognized by the network. Another way is to monitor network traffic and fish out the authorized MAC addresses.

Denial of Service Attacks: DoS attacks may be launched merely as a form of vandalism, to prevent legitimate users from accessing the network, or they may be carried out to provide cover for another type of attack. In Layer 1 DoS attacks, the hacker uses a radio transmitter to jam the network by emitting a frequency in the 2.4GHz or 5GHz spectrum. As 802.11 equipment operates at a certain signal-to-noise ratio, when the ratio drops below that threshold, the equipment will not be able to communicate.

In a more common type of DoS attack, the hacker uses a laptop or PDA with a wireless NIC to issue floods of associate frames to take up all available client slots in the AP, severing the AP's association with legitimate users. Alternatively, the hacker issues floods of de-association frames, forcing clients to drop their association with the AP. Either way, if the attack is successful, the hacker now controls access to the network.

Malicious Association: The hacker configures his device to behave as a functioning AP. When a user's laptop or station broadcasts a probe for an AP, it encounters the hacker's device, which responds with an association. At this point, the legitimate user's computer can be mined for any and all information, including MAC address, SSID, pass codes, etc.

Man-in-the-Middle Attacks: The hacker sends a de-authorization to a network device, which drops its association to its AP and begins searching for a new AP. It finds the hacker's station (configured to look like an AP), and associates with it. Using the information garnered from the legitimate device, the hacker's device now associates with the legitimate network AP and the network passes through the rogue user's device, allowing him to change or steal data at will.

Safeguarding The WLAN

NIST recently issued recommendations for securing the WLAN and other wireless connections, such as Bluetooth (an open specification using the globally available

2.4 GHz frequency to enable short-range wireless connections) and handheld devices.[9] NIST recommendations include:

- Maintaining a full understanding of the topology of the wireless network.
- Labeling and keeping inventories of the fielded wireless and handheld devices.
- Creating frequent backups of data.
- Performing periodic security testing and assessment of the wireless network.
- Performing ongoing, randomly timed security audits to monitor and track wireless and handheld devices.
- Applying patches and security enhancements.
- Monitoring the wireless industry for changes to standards to enhance to security features and for the release of new products.
- Vigilantly monitoring wireless technology for new threats and vulnerabilities.

In addition to these measures, AirMagnet recommends implementing a robust intrusion prevention system that will prevent attacks from getting underway in the first place.

Intrusion Prevention

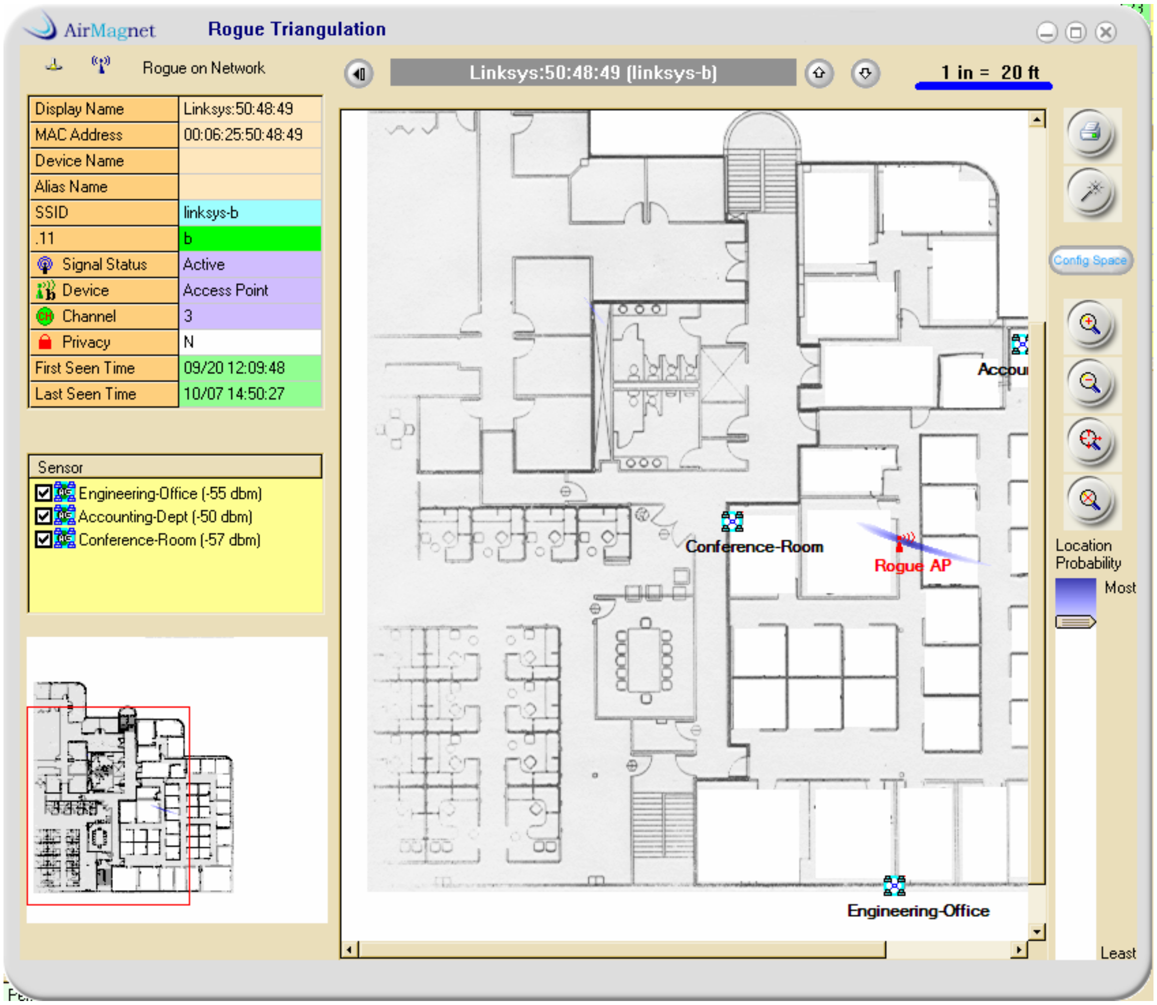
An effective intrusion prevention system monitors your WLAN to allow you to see what is happening in your airspace at all times, assures you that security policies

[9] "Wireless Network Security: 802.11, Bluetooth and Handheld Devices, Recommendations of the National Institute of Standards and Technology" Karygiannis, Tom and Owens, Les, NIST Special Publication 800-48, U.S. Dept. of Commerce, Gaithersburg, MD

are being followed, sounds the alarm when an intrusion or policy violation is detected, and isolates and cuts off any unauthorized device or user. Wireless LAN infrastructure devices come with some built-in monitoring capabilities, but a specialized overlay monitoring product will provide a richer set of capabilities.[10]

Detecting rogue and/or neighboring APs associated with your WLAN is essential. Once detected, it is critical to be able to physically locate these APs and take them out (or go have a polite discussion with the administrator of the neighboring WLAN). Locating a rogue AP requires triangulation, made possible by physically locating intelligent sensors around the area covered by the WLAN. Intelligent sensors detect the rogue AP or user, sound the alarm to the network administrator, and isolate the AP until it can be physically removed.

[10] "Watching the Waves," *Network Computing*, Mar. 4, 2004



Display Name	Linksys:50:48:49
MAC Address	00:06:25:50:48:49
Device Name	
Alias Name	
SSID	linksys-b
.11	b
Signal Status	Active
Device	Access Point
Channel	3
Privacy	N
First Seen Time	09/20 12:09:48
Last Seen Time	10/07 14:50:27

Sensor

☑ Engineering-Office (-55 dbm)
☑ Accounting-Dept (-50 dbm)
☑ Conference-Room (-57 dbm)

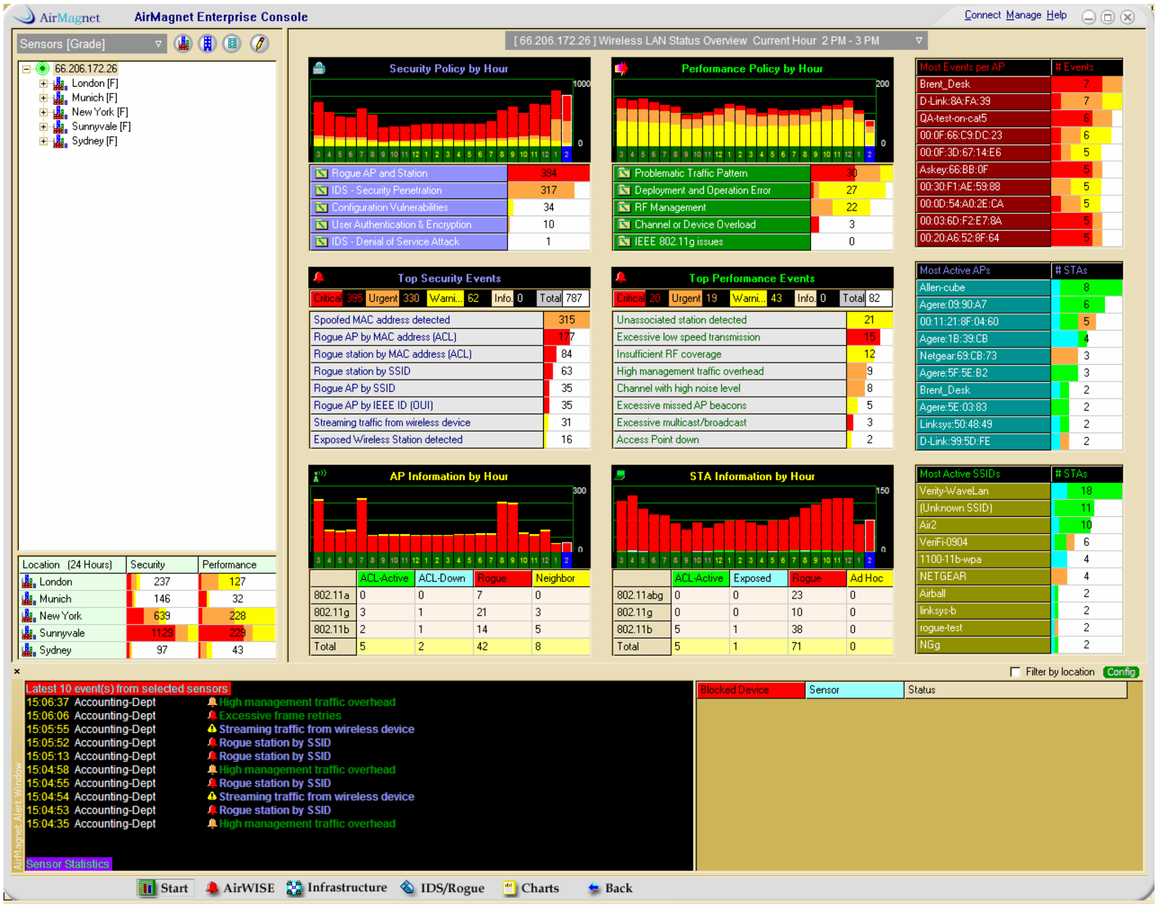
Triangulating Rogue APs. *A screenshot from AirMagnet Enterprise™ shows how AirMagnet's intelligent wireless sensors distributed around the WLAN triangulate and pinpoint the location of a rogue AP. Once the rogue's physical location is known, it can be removed without delay.*

Intelligent remote sensors can also monitor users/devices and determine whether a user is inside or outside your network perimeter. If a user is outside the perimeter –– whether the rogue user is a hacker or a neighbor who has unwittingly associated with your WLAN — the sensor will generate an alarm and isolate the rogue from the network.

One of the most useful aspects of a robust intrusion prevention system is the ability to set security protocols, and modulate the system's response to protocol violation. For instance, the system response to a low-level violation such as multipath detection, which could be merely a malfunctioning AP, might be just an email notification to the administrator, or a log notation. But a high level violation such as a user detected outside the network perimeter might result in a phone call alert.

It's essential to be able to manage WLAN security from a centralized console, where all information is quickly available to the administrator. The system should provide detailed information, such as activity at any single sensor, specifics on any alarm, and a view of network traffic at any given time. Troubleshooting tools, detailed logs, and the ability to measure network performance against established standards are all necessary to good network security. It is especially important to get reports in highly granular detail, customized to the needs of the network administrator. These reports are key to studying network performance and usage over time, pinpointing and eliminating potential trouble spots *before* they become problems.

And the network administrator needs flexibility from an intrusion prevention system. In many government agencies and organizations, access to information is strictly assigned on a need-to-know basis. Some government employees with top security clearance need access wherever they may be, while others may have access only while they are within specified physical locations. For instance, access privileges granted to a top-level executive need to travel with that person when he or she works from home or leaves on a business trip. A lower-level budget analyst may be allowed access only when he is located at a designated workstation. The system administrator must be able to configure related alarms into a coordinated policy instead of being limited to a fixed hierarchy. When the network is expanded, the intrusion prevention system must be scaleable to grow with it.



Security Policy by Hour	
Rogue AP and Station	394
IDS - Security Penetration	317
Configuration Vulnerabilities	34
User Authentication & Encryption	10
IDS - Denial of Service Attack	1

Performance Policy by Hour	
Problematic Traffic Pattern	30
Deployment and Operation Error	27
RF Management	22
Channel or Device Overload	3
IEEE 802.11g issues	0

Most Events per AP	# Events
Brent_Desk	7
D-Link:8A:FA:39	7
QA-test-on-cat5	6
00:0F:66:C9:DC:23	6
00:0F:3D:67:14:E6	5
Askey:66:BB:0F	5
00:30:F1:AE:59:88	5
00:0D:54:A0:2E:CA	5
00:03:6D:F2:E7:8A	5
00:20:A6:52:8F:64	5

Top Security Events

Critical	395	Urgent	330	Warni...	62	Info.	0	Total	787

Spoofed MAC address detected	315
Rogue AP by MAC address (ACL)	177
Rogue station by MAC address (ACL)	84
Rogue station by SSID	63
Rogue AP by SSID	35
Rogue AP by IEEE ID (OUI)	35
Streaming traffic from wireless device	31
Exposed Wireless Station detected	16

Top Performance Events

Critical	20	Urgent	19	Warni...	43	Info.	0	Total	82

Unassociated station detected	21
Excessive low speed transmission	15
Insufficient RF coverage	12
High management traffic overhead	9
Channel with high noise level	8
Excessive missed AP beacons	5
Excessive multicast/broadcast	3
Access Point down	2

Most Active APs	# STAs
Allen-cube	8
Agere:09:90:A7	6
00:11:21:8F:04:60	5
Agere:1B:39:CB	4
Netgear:69:CB:73	3
Agere:5F:5E:B2	3
Brent_Desk	2
Agere:5E:03:83	2
Linksys:50:48:49	2
D-Link:99:5D:FE	2

Location (24 Hours)	Security	Performance
London	237	127
Munich	146	32
New York	639	228
Sunnyvale	1129	229
Sydney	97	43

AP Information by Hour

	ACL-Active	ACL-Down	Rogue	Neighbor
802.11a	0	0	7	0
802.11g	3	1	21	3
802.11b	2	1	14	5
Total	5	2	42	8

STA Information by Hour

	ACL-Active	Exposed	Rogue	Ad Hoc
802.11abg	0	0	23	0
802.11g	0	0	10	0
802.11b	5	1	38	0
Total	5	1	71	0

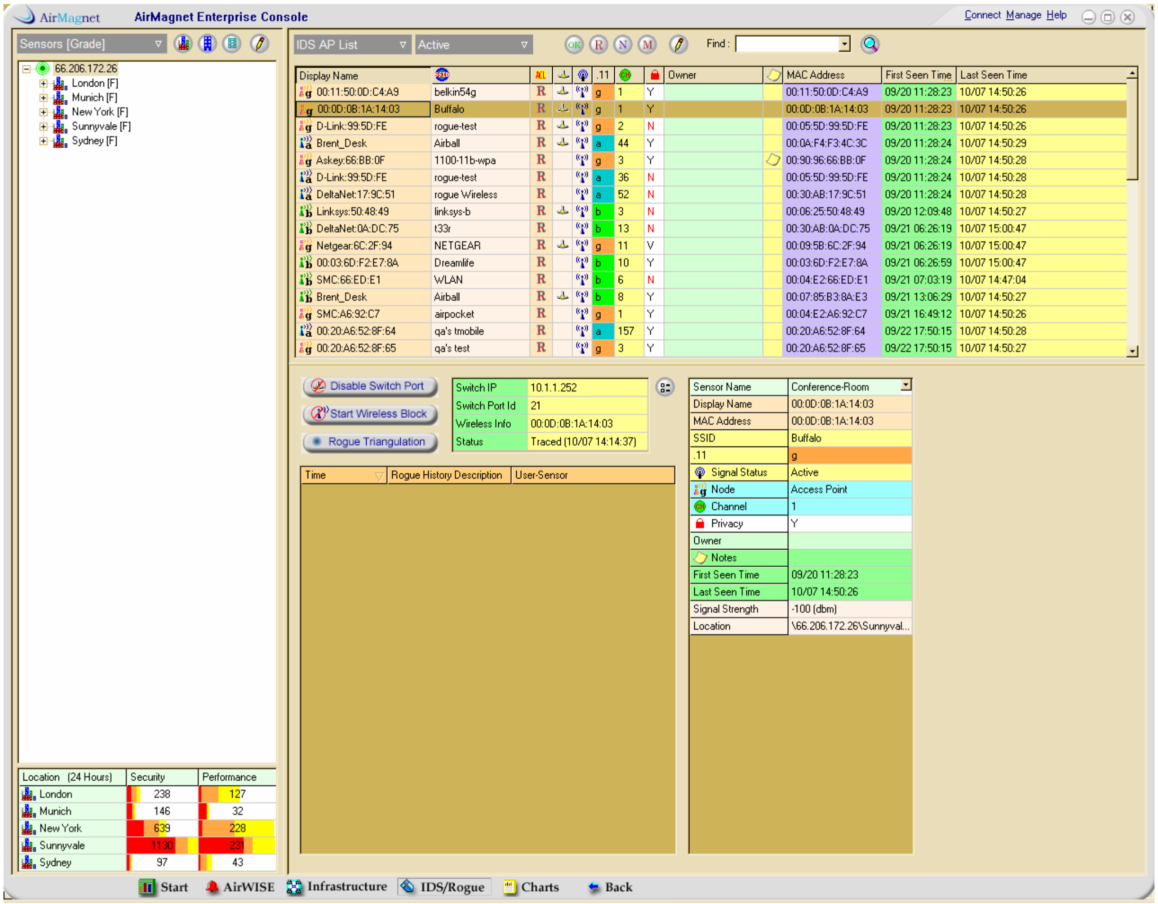
Most Active SSIDs	# STAs
Verity-WaveLan	18
(Unknown SSID)	11
Air2	10
VeriFi-0904	6
1100-11b-wpa	4
NETGEAR	4
Airball	2
linksys-b	2
rogue-test	2
NGg	2

```
Latest 10 event(s) from selected sensors
15:06:37 Accounting-Dept    High management traffic overhead
15:06:06 Accounting-Dept    Excessive frame retries
15:05:55 Accounting-Dept    Streaming traffic from wireless device
15:05:52 Accounting-Dept    Rogue station by SSID
15:05:13 Accounting-Dept    Rogue station by SSID
15:04:58 Accounting-Dept    High management traffic overhead
15:04:55 Accounting-Dept    Rogue station by SSID
15:04:54 Accounting-Dept    Streaming traffic from wireless device
15:04:53 Accounting-Dept    Rogue station by SSID
15:04:35 Accounting-Dept    High management traffic overhead
```

Blocked Device	Sensor	Status

***24/7 Monitoring.** The AirMagnet Enterprise™ console shows WLAN activity throughout the day. The system administrator can see at a glance which alarms have been given and when they occurred, traffic patterns, network performance and more. The system's granulation is very fine, allowing the administrator to analyze network activity and performance at many different levels.*

Intrusion prevention is enhanced if the system has mobile detection ability. Wireless LANs are constantly in a state of flux by their very nature. Users move around from location to location. New devices can introduce RF signals that didn't exist the day before. Users can create dead spots in the network without realizing it. For all these reasons, it is sometimes necessary to be able to make an on-the-spot investigation with a handheld extension of the intrusion prevention system that can perform real time readings and analysis.



- 66.206.172.26
  - London [F]
  - Munich [F]
  - New York [F]
  - Sunnyvale [F]
  - Sydney [F]

Display Name	SSID	ACL	⏚	📡	.11	CH	🔒	Owner	🗒	MAC Address	First Seen Time	Last Seen Time
00:11:50:0D:C4:A9	belkin54g	R	⏚	📡	g	1	Y			00:11:50:0D:C4:A9	09/20 11:28:23	10/07 14:50:26
00:0D:0B:1A:14:03	Buffalo	R	⏚	📡	g	1	Y			00:0D:0B:1A:14:03	09/20 11:28:23	10/07 14:50:26
D-Link:99:5D:FE	rogue-test	R	⏚	📡	g	2	N			00:05:5D:99:5D:FE	09/20 11:28:23	10/07 14:50:26
Brent_Desk	Airball	R	⏚	📡	a	44	Y			00:0A:F4:F3:4C:3C	09/20 11:28:24	10/07 14:50:29
Askey:66:BB:0F	1100-11b-wpa	R		📡	g	3	Y		🗒	00:90:96:66:BB:0F	09/20 11:28:24	10/07 14:50:28
D-Link:99:5D:FE	rogue-test	R		📡	a	36	N			00:05:5D:99:5D:FE	09/20 11:28:24	10/07 14:50:28
DeltaNet:17:9C:51	rogue Wireless	R		📡	a	52	N			00:30:AB:17:9C:51	09/20 11:28:24	10/07 14:50:28
Linksys:50:48:49	linksys-b	R	⏚	📡	b	3	N			00:06:25:50:48:49	09/20 12:09:48	10/07 14:50:27
DeltaNet:0A:DC:75	t33r	R		📡	b	13	N			00:30:AB:0A:DC:75	09/21 06:26:19	10/07 15:00:47
Netgear:6C:2F:94	NETGEAR	R	⏚	📡	g	11	V			00:09:5B:6C:2F:94	09/21 06:26:19	10/07 15:00:47
00:03:6D:F2:E7:8A	Dreamlife	R		📡	b	10	Y			00:03:6D:F2:E7:8A	09/21 06:26:59	10/07 15:00:47
SMC:66:ED:E1	WLAN	R		📡	b	6	N			00:04:E2:66:ED:E1	09/21 07:03:19	10/07 14:47:04
Brent_Desk	Airball	R	⏚	📡	b	8	Y			00:07:85:B3:8A:E3	09/21 13:06:29	10/07 14:50:27
SMC:A6:92:C7	airpocket	R		📡	g	1	Y			00:04:E2:A6:92:C7	09/21 16:49:12	10/07 14:50:26
00:20:A6:52:8F:64	qa's tmobile	R		📡	a	157	Y			00:20:A6:52:8F:64	09/22 17:50:15	10/07 14:50:28
00:20:A6:52:8F:65	qa's test	R		📡	g	3	Y			00:20:A6:52:8F:65	09/22 17:50:15	10/07 14:50:27

Switch IP	10.1.1.252
Switch Port Id	21
Wireless Info	00:0D:0B:1A:14:03
Status	Traced (10/07 14:14:37)

Time	Rogue History Description	User-Sensor

Sensor Name	Conference-Room
Display Name	00:0D:0B:1A:14:03
MAC Address	00:0D:0B:1A:14:03
SSID	Buffalo
.11	g
Signal Status	Active
Node	Access Point
Channel	1
Privacy	Y
Owner	
Notes	
First Seen Time	09/20 11:28:23
Last Seen Time	10/07 14:50:26
Signal Strength	-100 (dbm)
Location	\66.206.172.26\Sunnyval...

Location (24 Hours)	Security	Performance
London	238	127
Munich	146	32
New York	639	228
Sunnyvale	1130	231
Sydney	97	43

The Three D's of Intrusion Prevention. *Any wireless network can be threatened by rogue devices. The key to preventing intrusion by rogues is the ability to Detect, Disable, and Document every rogue before it can cause any damage. AirMagnet Enterprise provides a complete approach to rogue management including: multiple detection mechanisms that immediately expose every rogue; an active blocking suite that disables the rogue both on the wireless and wired side; and a dedicated rogue page that provides consolidated details on every device, including its physical location on a map, wired trace analysis, event history and more.*

Security Policy

There is no technology so sophisticated that human beings can’t mess it up. This is particularly true of WLAN security, because users outside the IT department often don’t realize that their actions may endanger the organization. A publications manager may know a great deal about printing and binding, but may be unaware that his or her laptop is not securely configured, even though the manager has used the proper passwords and procedures to gain remote access to the WLAN.

So WLAN user education is an important leg on the security stool. Users need to know about security protocols and how to follow them. More critically, users need to know *why* these protocols exist. Some people believe that rules are made to be broken. Understanding that the use of a rogue AP may enable a hacker to access sensitive data (or steal the user’s bank account number and identity), goes a long way toward gaining user compliance.

Every government organization with WLAN technology must develop a serious user training program to assure that users understand that they each have a personal responsibility to keep the organization safe from intrusion. Part of that educational process is setting protocols for securing laptops and other wireless devices and banning unauthorized APs.

AirMagnet Enterprise: A Complete Security System For The Government WLAN

AirMagnet Enterprise tames the complexity and exposure of a government WLAN with a true zero-tolerance approach to wireless security that is tied to the policies and needs of your organization. AirMagnet Enterprise detects every threat in the network, worldwide, and then automatically takes action with multiple layers of automated threat response. An intuitive global interface provides full disclosure of all wireless events, making it easy to make the right decisions while cutting through the time required to manage your networks. The end result is a system that brings simplicity, accountability, and bullet proof defenses to any wireless investment.

AirMagnet Enterprise SmartEdge Sensor software algorithms are compliant with the Federal Information Processing Standard (FIPS) 140-2 standard according to the NIST.

Detection

AirMagnet Enterprise automatically detects and alarms dozens of types of wireless intrusions, including rogue APs, DoS attacks, spoofed MAC addresses, the use of freeware probing tools and much more.

Prevention

AirMagnet Enterprise gives an alarm appropriate to the detected problem, but automatically moves to isolate and cut off rogue APs and rogue devices before the network is successfully penetrated. Multiple detection mechanisms identify rogues on the basis of MAC address, vendor type, wireless band or SSID. When the system operator arrives on the scene, AirMagnet Enterprise provides tools to physically locate suspect devices so they can be physically removed.

Vulnerability Assessment

WLANs are never static. Because they change from day to day, AirMagnet Enterprise performs a continuous vulnerability assessment of the network, detecting a host of subtle weaknesses that could result in network penetration. The system alerts IT immediately when it detects a vulnerability.

Control Over Security Policy

Even one AP or station that does not adhere to security policies puts the entire WLAN at risk. AirMagnet allows you to deploy different security strategies for different individuals or different locations, and monitor for 100% compliance. AirMagnet Enterprise offers 120+ security and performance alerts organized into a logical hierarchy, allowing managers to create and manage a coordinated policy. Each policy level and alarm comes with expert explanation and advice. Alarm notifications can be set to escalate in urgency if a problem gets worse.

About AirMagnet

Founded in 2001, AirMagnet, Inc., provides the most trusted WLAN management and security software systems in handheld, laptop and distributed configurations. Used by IT professionals at more than 2,600 organizations worldwide in government, manufacturing, financial, retail, service, health care, utility, transportation, and education sectors, AirMagnet solves Wi-Fi connection problems, tracks down unauthorized access, simplifies site surveys, and locks in unprecedented levels of network performance, security and reliability. Additional information about AirMagnet and its products is available on the Web at www.AirMagnet.com.

Agencies should understand that maintaining a secure wireless network is an ongoing process that requires greater effort than for other networks and systems. Moreover, it is important that agencies more frequently assess risks and test and evaluate system security controls when wireless technologies are deployed.
— National Institute of Standards and Technology[11] (NIST)

[11] "Wireless Network Security: 802.11, Bluetooth and Handheld Devices, Recommendations of the National Institute of Standards and Technology" Karygiannis, Tom and Owens, Les, NIST Special Publication 800-48, U.S. Dept. of Commerce, Gaithersburg, MD