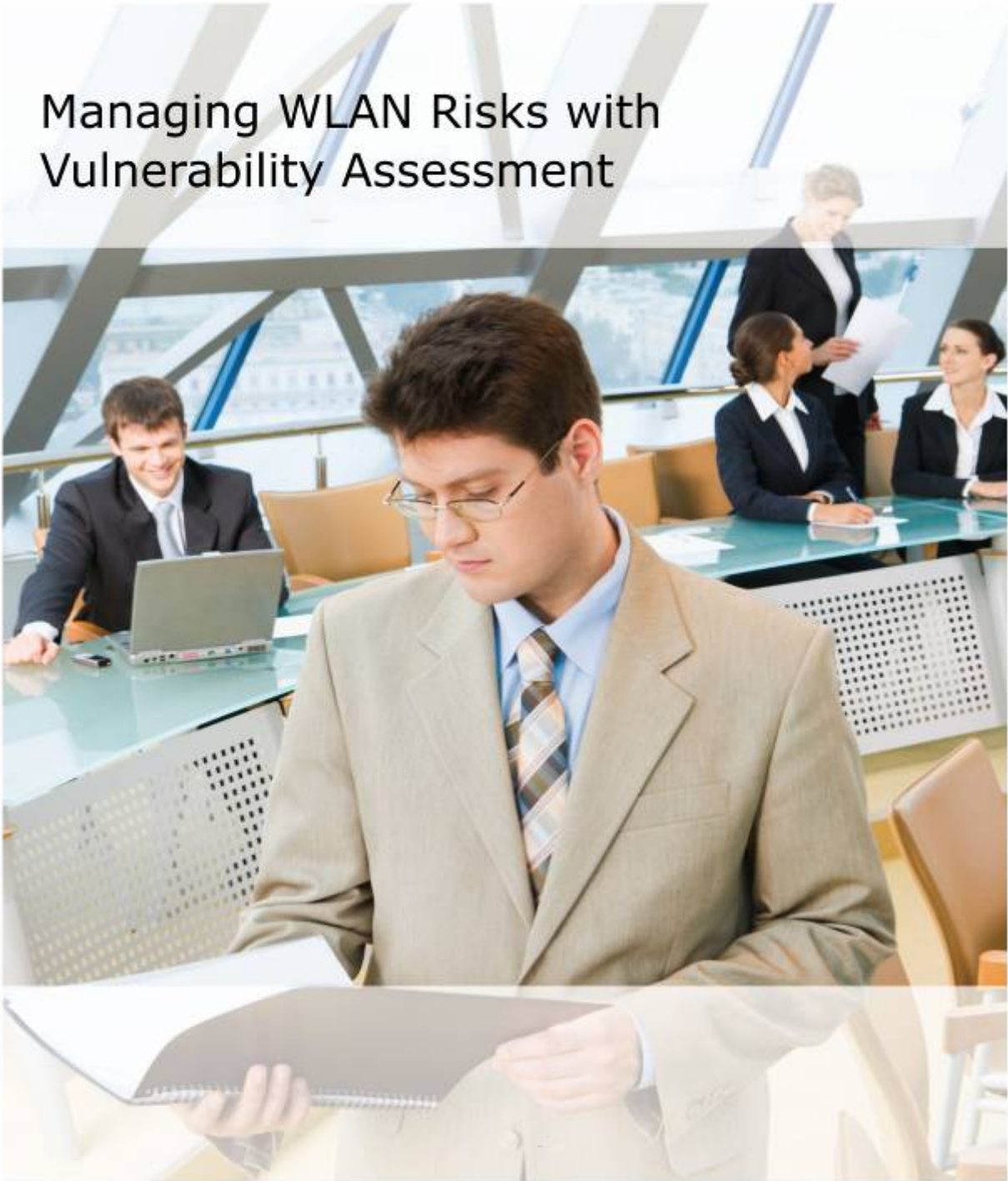


Managing WLAN Risks with Vulnerability Assessment



By Lisa Phifer
Core Competence, Inc.



Table of Contents

Summary	3
Managing WLAN Risks with Vulnerability Assessment	3
Understanding WLAN Vulnerabilities	3
Putting Attacks into Perspective: Risk Analysis	7
Conducting a Vulnerability Assessment	8
Putting Assessment Results to Work	12
How AirMagnet Can Help	13
Appendix A: Example Worksheet.....	18
About AirMagnet.....	22
About Core Competence	22

Summary

Many options are available to safeguard wireless LANs, but which security measures should your company deploy, and how can you tell whether your network is sufficiently hardened against 802.11 and 802.1X attacks? This paper describes an iterative process for business risk analysis, vulnerability identification, and threat remediation. It explains how to conduct your own WLAN vulnerability assessment to manage your risk, and how AirMagnet products can be used to make this process more efficient and effective.

Managing WLAN Risks with Vulnerability Assessment

With completion of 802.11i and maturation of Wi-Fi products, businesses now have the tools needed to safeguard wireless LANs, deflecting and reacting to intrusions. But enabling a few security options is not enough to provide the defense and in-depth security approach required in today's business critical Wireless LAN deployments. How can you really know whether your network is sufficiently hardened against 802.11 and 802.1X attacks?

A proven-effective defense requires systematic identification and elimination of vulnerabilities that could be exploited to penetrate your network and compromise business assets. This paper categorizes WLAN attacks and defines an iterative process for risk analysis. It explains how to conduct a vulnerability assessment and use results to mitigate high-priority threats. By finding and fixing your own vulnerabilities before intruders do, you can tap wireless benefits without creating unacceptable business risk.

Understanding WLAN Vulnerabilities

All networks are vulnerable, but in wired networks, physical barriers reduce risk by limiting media access. Ethernet switches can be locked away in closets and offices, and unused jacks can be disabled. But in wireless networks, the medium is the air. Walls, doors, and floors reduce signal strength, but do not stop attacks launched from stairwells, lobbies, parking lots, or nearby buildings. These new vectors can be used to exploit vulnerabilities that are inherent to 802.11 and 802.1X.

Inability to Control Access

War drivers use shareware Stumblers and high-gain antennas to discover WLANs. Intruders frequently penetrate company networks by exploiting unauthorized "rogue" APs, installed by naïve employees inside the firewall. They also look for promiscuous wireless devices that are willing to associate with any other device. Once connected, intruders can use traditional network attacks to probe clients, servers, and datastores to find open ports and exploitable services.

Careful AP placement can reduce RF signal leakage, but it won't stop outsiders from transmitting or receiving on channels used by your WLAN. Since access to the unlicensed bands used by 802.11 cannot be controlled, you must assume that both attackers and neighboring devices are present and "harden" wireless-connected devices to reduce interference and intrusion.

Lack of Confidentiality

Intruders discover your WLAN can easily eavesdrop on wireless traffic. Shareware or commercial capture tools can record packets and extract TCP/IP headers, usernames, passwords, email, files, voice calls, and anything else sent over the air. To inhibit eavesdropping, WLANs can encrypt 802.11 data frames using the Wired Equivalent Privacy (WEP) protocol, the Temporal Key Integrity Protocol (TKIP), or the Advanced Encryption Standard (AES) Counter Mode CBC Protocol (CCMP).

Unfortunately, all three protocols are vulnerable to static key cracking. Intruders can analyze captured packets to guess any WEP key or short, simple TKIP/AES Pre-Shared Keys (PSKs), using them to decrypt 802.11 Data packets. Cracking can be avoided by using TKIP and AES with long, complex PSKs or (better yet) dynamic session keys delivered via 802.1X. However, 802.11 Management and Control frames still cannot be encrypted, nor can header values like ESSID and MAC address. It is therefore important to know what attackers can see and assess the damage they can do with those values.

Users can also be tricked into associating with phony "Evil Twin" APs. By design, 802.11 stations roam automatically to the best AP with a given Extended Service Set Identifier (ESSID). Evil Twins lure users by Beaconsing the ESSID of a hotspot ("tmobile"), home ("linksys"), or corporate WLAN. Once associated to a victim, the Evil Twin is perfectly positioned to launch traditional Man-in-the-Middle attacks. By operating invisibly between the user and intended destination, an Evil Twin can easily solicit credit card numbers, inject viruses into web and email responses, or intercept data sent through "secure" tunnels to SSL or SSH servers.

Unauthorized Network Use

In networks that use WEP, WLAN access is controlled by a WEP key – a hexadecimal value known to all users. In networks that use TKIP or AES, access can be controlled by a PSK – an alphanumeric password known to all users. These shared keys grant everyone in a home or small business the same WLAN access. But an outsider who is told or guesses your WLAN's key gains full access to your network, just like everyone else.

Most businesses prefer to authorize WLAN access to individuals, based on authenticated user identity. With TKIP or AES, this can be accomplished using 802.1X Port Access Control. 802.1X carries the Extensible Authentication Protocol (EAP), messages used to validate identity by password, token, or digital certificate. Dynamic session keys are delivered to authorized users, while all other access attempts are rejected. However, some EAP types have vulnerabilities. For example, Lightweight EAP (LEAP) can be dictionary-attacked to obtain user passwords. Assessing your WLAN's 802.1X/EAP vulnerabilities can help you make safer choices.

Some businesses apply higher-level authentication at VPN gateways or application servers. But open WLANs – particularly hotspots – offer ample opportunity to capture or crack weak or exposed credentials like email logins, PPTP password hashes, and weak IPsec shared secrets. Finding and mitigating these authentication vulnerabilities can further help you deter unauthorized use of wireless-connected assets.

Forged Messages

All 802.11 packets carry a Cyclic Redundancy Check (CRC) that lets the receiver overcome transmission errors, but cannot stop forged frames with valid CRCs. To mitigate this vulnerability, TKIP and AES use sequencing and cryptographic message authentication to detect and discard injected or replayed 802.11 data packets. However, there is no standard to detect spoofed 802.11 management/control or 802.1X/EAP Start/Logoff packets. Raw packet injection tools can be used to send these spoofed packets at any time, launching numerous WLAN attacks -- especially DoS attacks.

Denial of Service

Cordless phones, Bluetooth, microwave ovens, neighboring APs, and metro-area WLANs all compete with your network, inhibiting service delivery. In fact, generating a high volume of spoofed 802.11 or 802.1X packets will impede legitimate WLAN use. DoS attackers may transmit continuously to prevent others from transmitting, flood the air with thousands of bogus AP Beacons, or send forged Deauthenticate, Disassociate, or EAP Logoff frames to stop users from staying connected. You cannot prevent outsiders from using the same unlicensed spectrum as your WLAN, but you can spot and react to this kind of unintended interference or malicious attack.

Other DoS attacks work by crippling wireless devices. For example, receiving a few bad TKIP data packets can trip an AP's invalid message threshold, suspending WLAN service for one minute. A malformed EAP-Identity response can crash APs that are vulnerable to this EAP-of-Death attack. Wireless devices are often new products that still need to be hardened against these and other DoS attacks.

Vulnerable Stations

As WLAN security protocols improved, attackers focused more attention on 802.11 stations. Many client devices are over-friendly by default, willing to associate with any other device, including unknown APs and Ad Hoc peers. This promiscuous behavior exposes both the station and your network to a multitude of risks, from unintentional file sharing with strangers to client bridging of traffic between public and private LANs.

In addition, numerous code flaws have been identified in wireless devices and 802.11 drivers. For example, exploits have been developed to trigger buffer overflows in 802.11 stations that do nothing more than passively listen for AP Beacons. Upon receipt, vulnerable stations may crash, or they may be used to execute malicious code. Vendors fix these bugs soon after they are discovered, many users don't keep up with patches, and new bugs are being found all the time. Auditing 802.11 station software and settings can help you take steps to mitigate these client-side vulnerabilities.

Table 1 summarizes common 802.11 and 802.1X attacks, giving examples of freely-available methods and tools used by wireless intruders. As we shall see, many of these tools can be used during an assessment to find your own vulnerabilities -- preferably before they can be exploited by others.

Category	Attack	Examples
Authentication Attacks Steal credentials to penetrate wired network and services	PSK Cracking	coWPAtty, Rainbow Tables
	LEAP Cracking	Anwrap, Asleep, LEAPcracker
	Password Capture	Dsniff, WinSniffer
	VPN Login Cracking	ike_crack, pptp_bruter
Access Control Attacks Circumvent filters and firewalls to obtain unauthorized access	War Driving	NetStumbler, WiFoFoFum
	MAC Spoofing	SMAC, MacChanger
	Rogue Access Points	WKnock, Draft 802.11n APs
	Unauthorized Ad Hocs	"Free Public WiFi" ESSID
Confidentiality Attacks Intercept sensitive or private data sent over wireless associations	Eavesdropping	Wireshark, Wellenreiter
	WEP Key Cracking	Aircrack-ptw, Chopchop
	Evil Twin	RGlueAP, 4-in-1 USB APs
	AP Phishing	Airsnarf, Hotspotter, KARMA
Integrity Attacks Modify packets sent over wireless to mislead attacker	802.11 / EAP Replay	Airpwn, wnet reinject
	802.11 / EAP Injection	Void11, LORCON
	Response Poisoning	Dsniff, MonkeyJack, Airpwn
Denial-of-Service Attacks Inhibit or prevent legitimate use of WLAN services	RF Jamming	Alchemy, HyperWRT
	Management/Control DoS	CTS-Jack
	Beacon Flood	FakeAP
	Deauth Flood	FATA-Jack, MDK2
	EAP-of-Death	Libradiate
Station Attacks Crash or compromise laptop, phone, or other Wi-Fi endpoint	Wireless Driver Exploits	Metasploit, LORCON
	Wireless Station Probes	WZCOOK, nmap

Table 1: Wireless LAN Attacks and Example Tools

Putting Attacks into Perspective: Risk Analysis

You can defend your WLAN from these attacks by using risk analysis to drive security policy definition and implementation. On-going monitoring and periodic testing can then be used to verify that a deployed WLAN meets defined objectives. Discovered vulnerabilities are then (re)analyzed so that policies can be refined and/or fixes can be applied. An iterative process like this (Figure 1) creates a concrete, measurable foundation for effective WLAN threat management.

Understanding the attacks that *can* occur is crucial. However, some attacks are less likely or more damaging than others. Furthermore, it is not practical or possible to defend any network against *all* possible attacks.

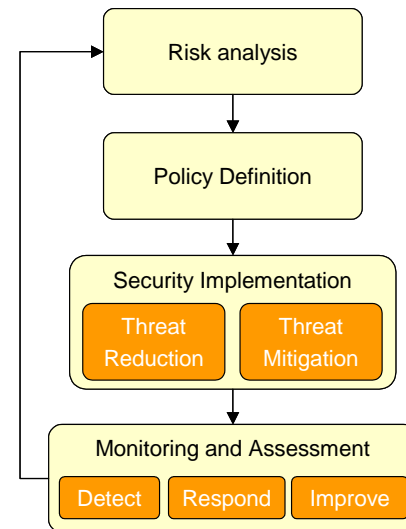


Figure 1:
Security As A Process

A more realistic goal is to *reduce* associated risk to an *acceptable level*. Put risks into perspective by identifying your own WLAN's vulnerabilities, the probability that attacker will exploit them, and the business impact should compromise occur. For example:

- Stumblers and WEP/PSK crackers help intruders gain wireless access to upstream networks. Wi-Fi enthusiasts often use these techniques simply to obtain free Internet access. In fact, most users accidentally associate with the wrong AP at some point. The *probability* that wireless service theft will be attempted is thus high. If your WLAN is open or lightly-secured, the *level of difficulty* is low. But what is the *business impact*? Stolen Internet access may be relatively benign -- unless used to launch more-damaging attacks. For example, WEP cracking led to the recent TJX break-in that compromised 45 million credit cards, at a cost of over \$1B. Breaches like this motivate many companies to focus on rogues that *actually connect* to the wired network or employee devices.
- An Evil Twin attack requires more interest and persistence than cleartext data capture. On the other hand, studies indicate that 9 out of 10 users connect to unknown WLANs, and business traffic at hotspots represents an especially lucrative target. Airport and hotel surveys routinely discover APs and Ad Hocs using tempting names like "Free Public WiFi." One might therefore rank Evil Twin attack as medium difficulty and probability. Consumers can take some comfort from credit card liability limits, but businesses must take steps to protect company assets from Evil Twin attacks -- for example, by requiring VPN tunnels at hotspots and mutual 802.1X authentication at the workplace.
- Point-and-click raw packet injection tools make 802.11 DoS attacks trivial, but what are the odds that one will be aimed at your WLAN? That depends on what the attacker gains; this may relate to business impact. Taking a conference room AP offline may result in little harm. But disabling an 802.11 surveillance camera could facilitate theft, while DoS-ing a hospital patient care WLAN could have dire consequences. These simple examples demonstrate why companies should spend more securing and monitoring their highest-priority WLAN assets.

To perform a risk analysis, start by defining business needs. Ultimately, security is not just about keeping intruders out – it's about letting legitimate users reach authorized services. Document who needs WLAN access, where. Identify users or groups permitted to use 802.11 at the office, on the road, and at home. Determine resources reached over wireless, like Internet destinations or corporate network segments. Which applications, databases, and shares must be opened to wireless users, and when?

Next, quantify new business risks caused by adding wireless. List the assets that will be put in harm's way on wireless and upstream wired networks. What information do those services and databases contain? Consider data that resides on wireless stations and flows over wireless links – this is also an asset to be protected. For each asset, estimate the likelihood of compromise and potential cost to your business, using quantifiable metrics like downtime, recovery expenses, breach notification costs, and the fines and criminal penalties incurred by a failed compliance audit.

When this process is complete, you will have a prioritized list of at-risk assets. Use this foundation to write a security policy that defends important assets from wireless-borne attack, balancing cost/benefit and residual risk. Then select, install, and configure counter-measures that implement and enforce that security policy. Finally, test your WLAN implementation to verify policy compliance and identify remaining vulnerabilities.

Conducting a Vulnerability Assessment

A vulnerability assessment is a systematic evaluation that uses penetration testing and observation to identify security weaknesses that could be exploited, and the consequences of doing so (e.g., attacks that run successfully, information they obtain, systems they compromise). These results are reviewed to determine severity and steps that reduce or eliminate threats -- for example, update an AP, reconfigure a client, add a firewall.

To be truly effective, assessments should be repeated. For example, conduct an assessment before and after initial WLAN deployment to spot newly-introduced vulnerabilities and verify that installed security measures are working as intended. Repeat the assessment after network upgrades or policy changes, and at regular intervals, to prevent vulnerabilities from creeping into your WLAN over time.

Assessments may be performed by in-house or third-party staff, with full, partial, or zero knowledge of your network and security implementation.

- In-house assessments can find and fix well-known vulnerabilities, before tapping outside expertise to spot unforeseen problems.
- Companies subject to regulations and laws like SOX or PCI DSS may be required to undergo periodic audits by qualified outside assessors.

All assessments should be conducted with the owner's consent, considering potential impact on business activities and network resources. For example, you may wish to perform DoS testing off-hours, but monitor WLAN activity 24/7 to support not only assessment, but audits and forensic investigation.

If you are responsible for conducting a WLAN vulnerability assessment, start by defining objectives, methodology, and expected outputs. Tests vary, depending upon available tools, the topology of the network being assessed, that network's security policy, etc. However, it is critical that the methods used, the tests run, and all results be documented to enable fix verification and consistent evaluation of the entire network.

Begin with a prototype assessment on a few WLAN resources, refining your methods and outputs until you are comfortable applying them on a larger scale. Use prototype results to revisit your objectives -- are you exercising the policy you intended to verify, or providing answers to the questions originally posed? This up-front "sanity check" can avoid wasting time on unnecessary tests or repetition to collect missing results.

The following sections discuss techniques and tools that can be useful when conducting a WLAN vulnerability assessment, from wireless device discovery and penetration testing, to security event monitoring and spectrum analysis. A sample worksheet, provided in Appendix A, illustrates how assessment results can be documented for review and remediation.

Using Portable Tools for WLAN Discovery

The first step in any vulnerability assessment is to identify all wireless devices near the site(s) under test. Authorized devices will be subjected to further assessment; the rest will be scrutinized to determine ownership, impact on WLAN operation, and potential threat. Discovery is part of the site survey conducted when planning a new WLAN, but the information needed for risk analysis is a subset of that required for RF network design. Here, we describe WLAN discovery for security purposes only.

Wi-Fi Stumblers are free, easy to use for simple tasks, and available for most Operating Systems, including handhelds. But they are also limited. Stumblers can find APs, but not Stations or non-802.11 interference sources. They may supply GPS latitude/longitude, but cannot pinpoint indoor location. A complete vulnerability assessment requires a portable WLAN Analyzer that can scan *all* RF channels, export details about *all* wireless devices, accurately *plot* results on floor plans, and make it easy to *find* newly-discovered devices.

For best results, work from a floor plan to methodically scan for devices at regular intervals, covering the entire site, inside and out, above and below. Scan all channels, in both RF bands, repeating the survey at least twice, at different times of day. Generate a list of observed 802.11 and other devices. For APs, record their ESSID, MAC address, IP address, channel, SNR, and observed 802.11/802.1X settings. Generate a similar list of discovered Stations, noting whether they are associated to an Ad Hoc node, probing for multiple ESSIDs, and/or actively associated with specific AP(s). For non-802.11 devices, use spectrum analysis to fingerprint type.

Next, use the site's WLAN inventory (if one already exists) to isolate previously-unknown devices. For efficiency, you may wish to list but otherwise ignore APs with weak SNR (distant neighbors) or transient unassociated Stations (guests). For the rest, use a "find" tool (or WIPS with rogue mapping) to locate each device, attempting to identify the equipment and owner. Finding all stations may not be practical – guest devices tend to be transient. But continue discovery until you have found all APs above a defined SNR and all significant interference sources.

Save scan results, using your assessment worksheet to consolidate what you have learned thus far. If possible, feed results into a WLAN planning system to visualize locations, overlapping coverage areas, and undesirable RF leakage. These results provide the foundation for penetration testing, inventory update, and Access Control Lists. For example, configuring your WLAN Analyzer with meaningful aliases and groups makes it easier to differentiate between authorized devices, known neighbors, and new rogues.

Using Penetration Tests to find Vulnerabilities

Intruders use wireless, TCP/IP, and server attack tools to compromise your WLAN. You can “fight fire with fire” by using these same tools to attempt to penetrate your own devices and WLAN infrastructure. Aiming simulated attacks at your WLAN determines whether intruders could successfully exploit common vulnerabilities, and helps you understand immediate consequences (e.g., visible data, networks breached, systems crashed).

Network-borne attacks usually scan devices and ports, using tools like Nmap or Superscan. Devices that appear to be active are “fingerprinted” to identify operating systems, server programs, accounts, and shares, using tools like Winfingerprint and Xprobe. A Common Vulnerabilities and Exposures (CVE) database is then consulted for flaws in the target's software and tools that can exploit them. During a WLAN assessment, aim these tools at your wireless gateways/switches, APs, hosts, and other systems exposed to wireless, like DHCP and DNS servers. Run tests while associated to different APs to spot subnet-specific vulnerabilities. If your WLAN uses VPN or portal authentication, runs tests both before and after authentication.

Intruders exploit active APs and open ports to connect to your network and services. Management ports (Telnet, SSH, SNMP, TFTP) may be probed, using default logins. WEP traffic may be analyzed with a tool like Aircrack-ptw, while PSK authentication messages may be analyzed with coWPAtty. 802.1X/EAP user IDs may be recorded and password-based EAPs may be tested using a tool like Asleep. During an assessment, use these tests to identify weak controls and credentials for every device/port and ESSID. To test off-hours, you may need to generate traffic, using a tool like iperf. You may need to be patient, because time-to-crack varies, depending on type of adapter, traffic, and password strength.

Intruders may also aim 802.11, 802.1X, and TCP/IP DoS tools at WLAN infrastructure. An assessment should therefore exercise your WLAN's DoS defenses, including configurable thresholds on wireless gateways, switches, and firewalls, and Wireless Intrusion Prevention System coverage. For example, go systematically from floor to floor, using tools like CTS-Jack and MDK2 to flood the target and find any WIPS sensor coverage holes. Use a framework like Metasploit to probe every AP model/version in your WLAN for product-specific DoS vulnerabilities by sending 802.11 and 802.1X exploit messages. Aim TCP, UDP, and ICMP floods at your WLAN gateway/firewall to find the rate at which failure (if any) occurs. Because DoS testing is disruptive -- and potentially destructive -- exercise caution about which tests you run, when, and where.

Finally, run your own Evil Twin AP and wireless driver exploits to assess how wireless stations react and evaluate the effectiveness of deployed countermeasures. For example, try various ESSIDs to lure stations that are vulnerable to Hotspotter attack. Run KARMA on an Evil Twin to identify application credentials that are easily intercepted. If you use WIPS to auto-block rogue APs, verify that your Evil Twin is effectively contained in this manner, testing at least two simultaneous rogues, with and without corporate network connectivity. Simulate rogue scenarios that can be a bit harder to spot, like draft 802.11n APs, lower power APs, and those tuned to unusual channels not normally used by your WLAN.

Many of the tools mentioned here can be individually downloaded from websites or found in a pen-test collection like BackTrack (www.remote-exploit.org). Use pen-test results to flesh out your assessment worksheet, highlighting attacks that were easy and had major impact. Include observations that may be helpful when determining fixes (e.g., visible RF obstructions).

Using WIPS to Monitor Activity

WLAN discovery and pen-tests find vulnerabilities, but do not tell us if those vulnerabilities have been exploited. Portable WLAN Analyzers can "spot check" wireless activity in one location -- in fact, running an analyzer next to your pen-test system can be helpful to eyeball simulated attacks. But for full-time monitoring of your entire WLAN, devices therein, and actual user traffic, use a Wireless Intrusion Prevention System (WIPS).

Like wired network IPS, a wireless IPS uses traffic analysis to watch for attack signatures, protocol errors, atypical behavior, and policy violations, generating alerts and defensive actions. But WIPS sensors listen to the air, in local and remote offices, decoding 802.11/802.1X protocols and analyzing all wireless activity within a given RF band. WIPS servers understand wireless attacks and can enforce wireless security policies -- for example, automatically deauthenticating rogue devices. Intrusion alerts and related evidence are recorded to a central database for future reference during routine compliance reporting or post-breach forensic analysis.

WIPS also can be extremely helpful during a WLAN vulnerability assessment. WIPS can help "fill in the blanks" during WLAN discovery, because a full-time monitor will inevitably hear more than ad hoc sampling. By combining observations made by several remote 802.11 and spectrum sensors, WIPS can triangulate a discovered device's location on a floor plan to make searches more efficient. By generating policy-based alerts, WIPS can help you spot misconfigured devices, actual attacks that may have occurred recently, problem-prone locations and devices that may warrant additional scrutiny, and on-going risky user behavior.

During pen-testing, WIPS can confirm that tests are working as expected. It can teach you how to recognize signs of attack. It can record information needed to investigate an incident or understand its impact, long after the attack ends. WIPS can even combine current and past observations to suggest how to mitigate threats. In return, pen-test results may help you fine-tune your WIPS. For example, results may lead you to adjust sensor placement, change scanned channels, augment 802.11b/g sensors with 802.11a/n and spectrum analysis, revise DoS alert thresholds, customize alert notifications, or extend WIPS data retention policies.

Using Wireless Analyzers for Investigation

The broad insights delivered by WIPS can be complemented by drill-down investigation. WLAN and spectrum analyzers are instrumental during vulnerability assessment, from start to finish. Portable (laptop or handheld-based) analyzers provide a mobile platform for device discovery, traffic capture, and eye-balling wireless activity while pen-tests are in progress. After testing ends, remote (WIPS sensor or AP-based) analyzers can help you dig deeper to investigate potential vulnerabilities.

For example, when pen-testing a site, you might use a handheld analyzer to capture and decode live 802.11 packets. By examining channel utilization, you spot a channel experiencing considerable RF interference. By drilling down with a handheld spectrum analyzer, you can identify the non-802.11 culprit (e.g., microwave oven) and narrow down its location.

Alternatively, if the poor air quality appears to be caused by 802.11 packet collisions, you might apply a filter to focus on suspicious traffic -- for example, all 802.11n packets. If the source is an unknown AP, you can try to associate with it and trace network connectivity. If the source is a hidden node, you can use a "finder" – an audio-visual real-time signal strength meter – to move towards the offending device. Wireless devices can be gone by the time assessment results are reviewed, so it is best to gather information during the test itself. But there will inevitably be situations where, during review, gathering further information could help. Remote analyzers fill that gap without traveling back to the test site. For example, you might instruct a WIPS sensor at the test site to record live transmissions, enabling drill-down spectrum analysis. At sites without dedicated WIPS sensors, you might place an AP into remote analyzer mode to see decode a suspicious station's traffic in real-time.

Why stock your pen-test toolbox with portable *and* remote WLAN *and* spectrum analyzers? Portable analyzers excel at efficient on-site investigation, while remote analyzers enable cost-effective off-site investigation. WLAN analyzers let you peer into 802.11, while spectrum analyzers dig into non-802.11 transmissions. In WLANs that carry voice over IP, VoFi analyzers can assess call impact. The combination gives you the best of all worlds, bypassing the limitations of any single analyzer.

Putting Assessment Results to Work

Wireless vulnerability assessments are a means to an end. To reduce business risk, results must be applied to eliminate vulnerabilities through station and AP hardening, rogue detection and elimination, and deployment of 802.11/802.1X security measures. Assessment reports should rank identified vulnerabilities by severity and recommend countermeasures.

Rogue Management: Most vulnerability assessments find at least some previously-unknown wireless devices. Assessment results enumerate discovered devices ("rogues") and observed properties to enable threat assessment, classification, and elimination. For example, a report might recommend classifying low-SNR APs as Neighbors so that ACLs be used to block unauthorized associations. It may recommend physical removal of discovered high-SNR APs connected to the corporate network without permission and stand-alone draft 802.11n APs installed by employees.

Proactive measures can also be recommended to prevent rogue damage in the future. For example, suspicious stations may be added to WIPS "watch list" to escalate any future alerts pertaining to them. Automated actions may be configured for malicious rogues that lie off-premises but within RF range, like network connectivity checks and temporary wireless blocking. After such measures are deployed, repeat assessments can verify effectiveness.

WLAN Infrastructure Hardening: APs, switches, gateways, web portals, DNS/DHCP servers, and other devices connected to WLANs often require hardening to resist network-borne attacks. Pen-test results may be accompanied by recommended countermeasures, like changing AP defaults, disabling unnecessary services, using stronger admin passwords or authentication methods, disabling wireless-side management and restricting wired-side to specific IP addresses and/or VLANs, adding AP filters to prevent route updates or LAN broadcasts from being relayed onto the wired network, tuning DoS thresholds, and applying firmware upgrades/patches. It may not be possible to eliminate all discovered

vulnerabilities while meeting business needs, but applied fixes should be verified through repeat testing until residual risk is acceptable.

Station Hardening: Wireless-enabled desktops, laptops, PDAs, scanners, cameras, printers, VoFi phones, and field terminals can also be hardened. Countermeasures and best practices typically used to defend Internet-connected hosts, like personal firewalls, are generally recommended for WLAN hosts. Pen-test results may also identify WLAN-specific vulnerabilities that warrant further recommendations, like configuring stations to make Infrastructure associations to corporate ESSIDs only, checking 802.1X server certificates to avoid Evil Twins. Wireless adapters that support only WEP might be retired, while those with vulnerable drives should be patched. If associations were found to neighbor or metro-network APs, user education and on-going surveillance may be recommended.

Securing Data In Transit: Assessments can verify compliance with your security policy and identify weaknesses in that policy. For example, if policy requires AES encryption on the corporate WLAN, test results should enumerate devices willing to associate without AES. Sensitive data sent without encryption on a guest WLAN might be documented to support risk analysis. If risk is too high, employee associations to the guest WLAN could be blocked, while guests might be advised to protect themselves with VPN tunnels. The report may recommend alternatives to reduce over-the-air vulnerabilities and comply with data privacy regulations.

Controlling Network Use: Finally, assessments exercise the WLAN's Access Control and Authentication mechanisms to determine whether and where and how breach can occur. Results may enumerate visible user identities and crackable credentials that should be strengthened. They may demonstrate unexpected consequences of compromise -- for example, other systems that can be accessed with cracked user credentials, or products with authentication-related CVEs. Here again, recommendations can be made to mitigate vulnerabilities, based on the WLAN's defined security policy. For example, if policy permits authentication by PSK, test results should enumerate ESSIDs with weak PSKs, recommending replacement with stronger PSKs or perhaps 802.1X. Tests should be repeated to verify changes and detect new vulnerabilities -- this is particularly true when upgrading to a relatively complex solution like 802.1X or a new EAP Type.

How AirMagnet Can Help

AirMagnet provides a comprehensive tool suite for on-site and off-site WLAN Vulnerability Assessment. From site surveys and spectrum analysis to remote security monitoring and WLAN analysis, AirMagnet products can help you conduct efficient, effective assessments to manage wireless risk.

AirMagnet Survey/Planner lets you visualize WLAN plans and site survey results in meaningful terms. Survey/Planner uses a floor plan to map the wireless devices discovered during site surveys, sharing this data easily with other AirMagnet products. On-site survey readings can be taken with AirMagnet Laptop or Handheld, operating in passive (listen only) or active (associate to AP) mode. All survey results – including Spectrum Analyzer measurements -- can then be merged within Survey/Planner to support WLAN planning, simulation, verification, and what-if optimization.

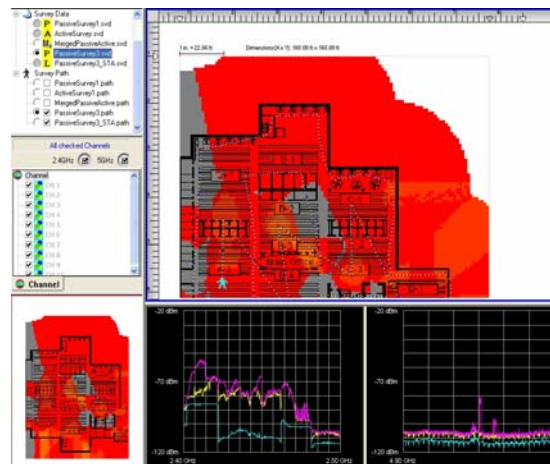


Figure 3: AirMagnet Survey/Planner

AirMagnet Spectrum Analyzer uses patented spectral fingerprinting techniques to measure, analyze, and display sources of RF interference in all 802.11 bands. Spectrum Analyzer can recognize devices that are adversely impacting your WLAN in real time, including Bluetooth, cordless phones, microwave ovens and analog video cameras. A built-in Device Finder tool can then be used to speed investigation and elimination. Spectrum Analyzer can run on any Windows laptop, or it can be invoked as a drill-down tool when using other AirMagnet products.

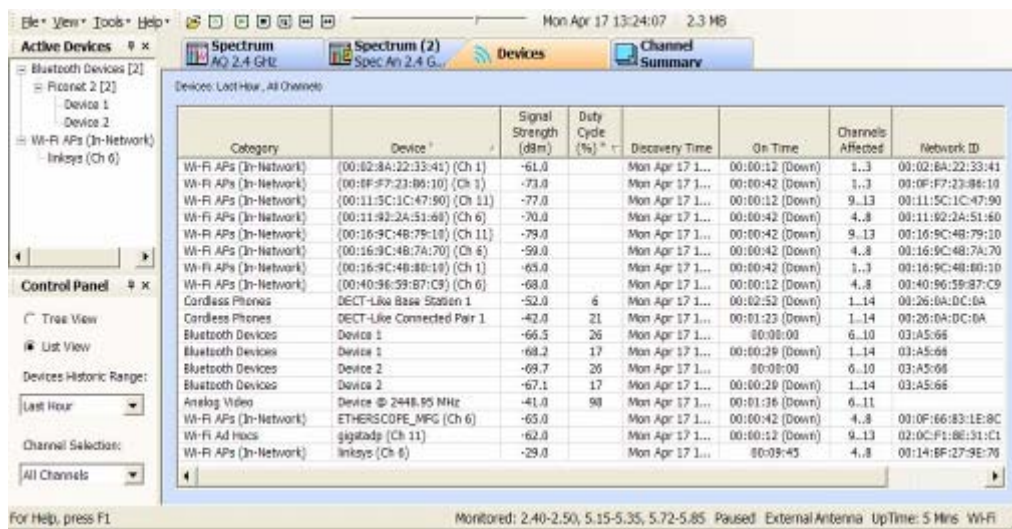


Figure 4: AirMagnet Spectrum Analyzer

AirMagnet WiFi Analyzer and **AirMagnet Handheld Analyzer** are portable platforms for WLAN traffic observation, capture, and analysis. They provide an extensive set of 802.11 monitoring and diagnostic tools to find wireless devices, document information about them, spot-check their activity, and trouble-shoot problems. AirMagnet Analyzers can scan all 20 and 40 MHz channels used by 802.11a, 802.11b/g and draft 802.11n devices, in the 2.4, 4.9, and 5 GHz band. They can filter and decode 802.11 traffic (including draft 802.11n) and use expert analysis to automatically identify attempted intrusions, weak configurations, and policy deviations.

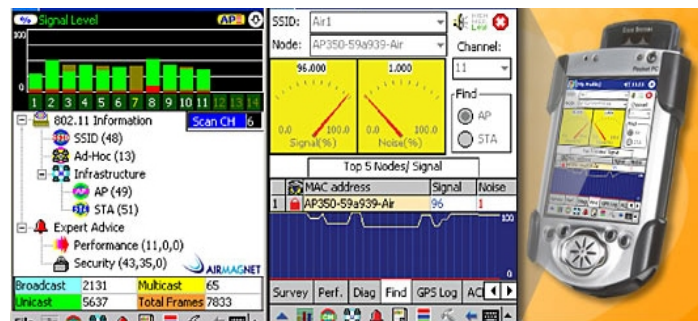


Figure 5: AirMagnet Handheld Analyzer

With an AirMagnet Analyzer, you can associate with a specific AP to check network connectivity and run targeted penetration tests. Results can be played back at a later time, exported to AirMagnet Survey/Planner, or fed into AirMagnet Enterprise in real-time. AirMagnet WiFi Analyzer PRO offers built-in, customizable compliance reports for SOX, Basel II, EU-CRD (Cad 3), ISO 27001, FISMA, HIPAA, PCI-DSS, DoD 8100.2, and GLBA, including step-by-step pass/fail verdicts for each section of these standards.

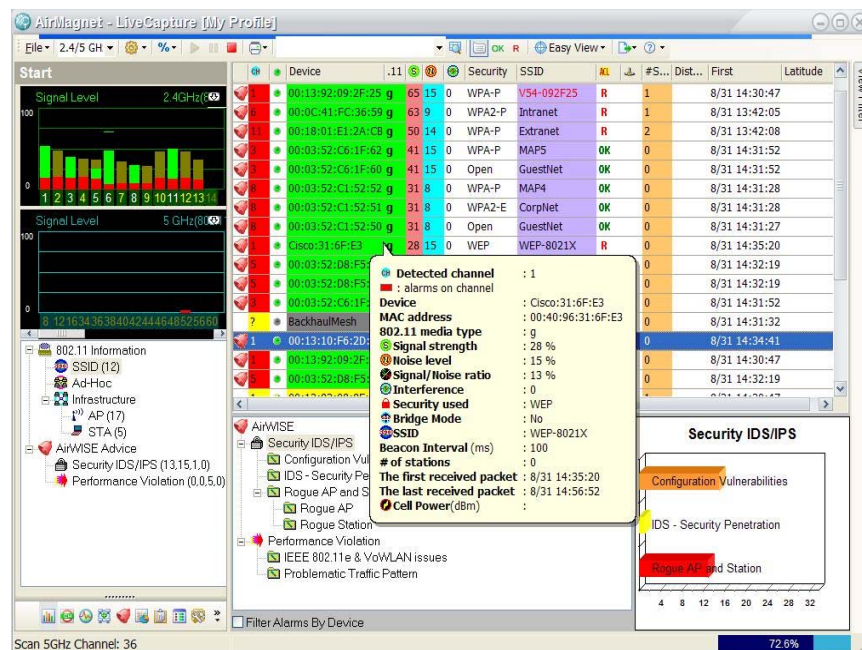


Figure 6: AirMagnet WiFi Analyzer

AirMagnet Enterprise Analyzers for Cisco and Aruba can enable remote WLAN analysis in Cisco Unified Wireless and Aruba Mobile Edge networks. Enterprise Analyzers interface with Cisco or Aruba controllers to temporarily convert ordinary APs into sensors. This permits analysis of real-time WLAN traffic, collected without on-site staff or dedicated WIPS hardware – for example, to close gaps when reviewing assessment results.

AirMagnet VoFi Analyzer is a specialized monitoring and trouble-shooting tool for Voice over Wi-Fi networks. This portable Analyzer can diagnose QoS, RF, WLAN, and wired network problems that impact voice calls. AirMagnet VoFi PRO integrates with voice solutions from Cisco, Spectralink and Vocera for complete end-to-end call analysis – for example, to complement 802.11 survey results with user names and phone numbers.

AirMagnet Enterprise delivers robust, scalable 24/7 wireless intrusion detection and prevention. By combining dedicated SmartEdge sensors with a fault-tolerant central server, Enterprise can spot over 130 wireless security, performance, and operational problems, recording incident data to support forensic analysis while automatically defending the network in real-time.

Potential Pre-802.11n Device Detected

Alarm Description & Possible Causes

In January 2004, the IEEE announced that it had formed a new 802.11 Task Group (TGn) to develop a new amendment for the existing standard for wireless local-area networks. It was expected to provide transmission speeds greater than 100 Mb/s, but this proposal has come a long way, with even higher speeds being possible at this time: it may even reach the theoretical value of 540 Mb/s. It is also expected to provide a larger range than the 802.11a/g standards and will operate in the 2.4 Ghz band shared with 802.11b/g devices.

Initially, there were two proposals to the standard:

- WWiSE (World-Wide Spectrum Efficiency), backed by companies such as Airgo, Broadcom, Conexant, and Texas Instruments, and
- TGn Sync, backed by Intel, Atheros, Marvell, Agere, and Philips.

#	ACL/SSID Group	Severity	Notification
1	MyWLAN	Warning	Beep

Policy Wizard Notification Wizard Reset

Figure 7: AirMagnet Enterprise Policy Management

An Enterprise server uses customizable policies to categorize and proactively respond to the events observed by SmartEdge 802.11 sensors, spectrum sensors, or even AirMagnet WiFi Analyzer, operating as a sensor. When a potential attack or weak configuration is found, Enterprise can launch active traces to determine where the device is attached to the network and map its location. Wired or wireless blocking can be invoked to neutralize the threat while buying time for investigation. Finally, to gather forensic evidence, Enterprise can record and retain a full packet capture, to be replayed at any time from the Enterprise console.



Figure 8: AirMagnet Enterprise

Finally, all of these AirMagnet products are integrated with each other. This makes it easy to share configured policies and test results, drill-down from one product to another, and use diagnostic tools and compliance reports consistently – whether running a test on-site or reviewing results off-site

Appendix A: Example Worksheet

The following worksheet illustrates how results gathered during a vulnerability assessment can be recorded. Just as there is no "one size fits all" testing process, there is no standard form to record these results. Use this example to create your own worksheet that reflects what you plan to test and monitor during your own vulnerability assessment. We recommend taking your worksheet on a "test drive" to ensure that documented results are complete and meet assessment objectives.

Test Date	
Tester MAC(s)	
Tester Adapter(s)	

Intended / Deployed WLAN Characteristics

AP	Number	Station	Number	Other	Number	Assigned ESSIDs
802.11b		802.11b		Micro waves		Employee Intranet =
802.11g		802.11g		Cordless Phones		Guest Intranet =
802.11a		802.11a		Bluetooth Devices		Other =
802.11n		802.11n		Video Cameras		
WLAN Bridges		Ad Hoc Stations		Other RF Sources		

Site Survey Floor Plan and Test Locations

1.	Insert Floor plan Here Mark Testing Locations on Floorplan Describe Testing Locations at left (Or generate from Survey/Planner as in Figure 3)
2.	
3.	
4.	
5.	

AP Inventory

AP MAC	ESSID	Ch#	IP Address	SNR	Owner	Location	Classification
: : : : :							
: : : : :							
: : : : :							

AP MAC	Protocol Types	SSID Beacon	802.11 Encrypt	PSK	802.1X	EAP Types	Other
: : : : :							
: : : : :							
: : : : :							

Station Inventory

STA MAC	Last ESSID	Last Ch#	SNR	Owner	Location	Adapter	Classification
: : : : :							
: : : : :							
: : : : :							

STA MAC	Protocol Types	Assoc ESSIDs	802.11 Encrypt	PSK	802.1 X	EAP Types	EAP User ID
: : : : :							
: : : : :							
: : : : :							

Network Scan Results: Discovered Devices (complete for each VLAN/Subnet)

Role	MAC Address	IP Address	Owner	Notes
WLAN Controller	: : : : :			
DHCP Server	: : : : :			
DNS Server	: : : : :			
RADIUS Server	: : : : :			
Access Points	: : : : :			
Stations	: : : : :			
Other	: : : : :			

AP Test Results (complete for each tested AP)

AP MAC	: : : : :	AP IP Address	
Virtual AP?		VLAN ID	
OS/Version			
Open TCP/UDP Ports		Service Banners Returned	
SNMP Admin Used?		SNMP Community Strings	
Telnet Admin Used?		Telnet Login / Password	
Web Admin Used?		Web Login / Password	
Blocks Broadcasts?		Blocks Station-to-Station?	
Blocks WLAN SNMP?		Blocks WLAN Routing?	
Accepts Spoofed ARP?		Physically Secured?	
Encryption Off?		Observed Encryption Types	
WEP Weak IVs?		Cracked WEP Keys	
MAC ACL Used?		Valid Station MACs	
PSK Guessable?		Cracked PSK	
802.1X Required?		Observed EAP Types	
AP DoS Test Results		RF Interference Sources	

Station Test Results (complete for each tested Station)

Station MAC	: : : : :	Static IP Address?	
OS/Version		VLAN ID?	
Open TCP/UDP Ports		Service Banners Returned	
NetBIOS Name		NetBIOS Shares	
NetBIOS Service List		NetBIOS User/Group List	
Assoc with ANY AP?		Assoc with Ad Hoc Peer?	
Encryption Off?		Observed Encryption Types	
WEP Weak IVs?		PSK Guessable?	
802.1X Used?		Observed EAP Types	
802.1X IDs Exposed?		Observed 802.1X User ID	
LEAP Used?		Cracked User Password	
Applications Protocols		Observed Servers & Logins	

WLAN Infrastructure Test Results**(complete for each tested controller/switch/server)**

Device MAC	: : : : :	Device IP Address	
OS/Version		VLAN ID	
Open TCP/UDP Ports		Service Banners Returned	
SNMP Admin Used?		SNMP Community Strings	
Telnet Admin Used?		Telnet Login / Password	
Web Admin Used?		Web Login / Password	
Accepts Spoofed ARP?		Physically Secured?	
Uses RADIUS Server?		RADIUS Test Results	
Acts as DNS Server?		DNS Test Results	
Acts as DHCP Server?		DHCP Test Results	
Acts as VPN Gateway?		VPN Test Results	
Acts as Web Portal?		Web Server Test Results	

Detected Attacks and Anomalies

Type of Event	Source Address	Dest Address	Time	Location	Observations and Details
Network DoS Attacks - CTS Flood - Queensland DoS - PS Poll Flood - Virtual Carrier Attack - RF Jamming - RF Spectrum Interference					
AP DoS Attacks - 802.11 Association Flood - 802.11 Authenticate Flood - 802.11 MIC DoS Attack - 802.1X EAP Start Flood - 802.1X EAP of Death - Fuzzing Attacks (Illegal 802.11 Packets)					
Station DoS Attacks - 802.11 Deauth Flood - 802.11 Deauth Broadcast - 802.11 Disassociate Flood - 802.11 Disassoc Broadcast - 802.1X EAP Failure - 802.1X EAP Logoff Flood - Wireless Driver Exploits - PSPF Violation					
Reconnaissance Activities - NetStumbler - Wellenreiter - FATA-Jack - AirSnarf - MAC Address Spoofing					
Evil Twin / MitM Activities - Fake AP Detected - Fake DHCP Server - Hotspotter Detected - SoftAP or HostAP - AP in Bridged Mode - Suspicious ESSIDs					
Spoofing / Cracking - MAC Spoofing - Fast WEP Crack Attack - ASLEAP Attack - EAP Dictionary Attack - EAP Type Attack					

This table summarizes Wireless IPS and WLAN analyzer security alerts corresponding to attacks and anomalies observed during the assessment period. Note: deviations from defined security policy and rogue devices should be recorded in the AP or Station List.

About AirMagnet

AirMagnet Inc. is the leader in security, performance and compliance solutions for wireless LANs. The company's innovative products include AirMagnet Enterprise, the leading 24x7 WLAN security and performance management solution, and AirMagnet WiFi Analyzer – which is known as the “de facto tool for wireless LAN troubleshooting and analysis.” Other products provide WLAN site survey and design, RF interference detection, remote diagnostics, and the world's first voice over Wi-Fi analysis solution. AirMagnet has more than 6,000 customers worldwide, including 75 of the Fortune 100. The company, based in Sunnyvale, Calif., has offices worldwide. For more information, visit www.AirMagnet.com.

About Core Competence

Core Competence, Inc. is a full-service network and security consulting firm with offices in Pennsylvania and South Carolina.

Lisa A. Phifer, Vice President, has been involved in the design, implementation, and evaluation of data communications, internetworking, security, and network management products for over 20 years. At Core Competence, she has advised companies large and small regarding security needs, product assessment, and the use of emerging technologies and best practices. Before joining Core Competence, Lisa won a Bellcore President's Award for her work on ATM Network Management. She teaches about wireless LANs, mobile security, and virtual private networking, and has written extensively for numerous publications, including Wi-Fi Planet, ISP-Planet, Business Communications Review, Information Security, and SearchSecurity. Lisa's WLAN Advisor column is published by [searchMobileComputing](http://searchMobileComputing.com).



Corporate Headquarters:

830 E. Arques Avenue
Sunnyvale, CA 94085
United States

Tel: +1 408.400.0200
Fax: +1 408.744.1250

EMEA Headquarters:

St Mary's Court
The Broadway
Amersham
Buckinghamshire, HP7 0UT
United Kingdom

Tel: +44 1494 582 023
Fax: +44 870 139 5156