

SELECTING A WLAN MONITORING SOLUTION

A Spire Research Report – December 2003

By Pete Lindstrom, Research Director



Spire Security, LLC
P.O. Box 152
Malvern, PA 19355
www.spiresecurity.com

Executive Summary

There is no denying the utility of wireless networking. As access points pop up throughout an enterprise and in “hot spots” around the world, security becomes a primary theme. One approach to security is to apply trust mechanisms, such as authentication and WEP encryption, to the environment. While this security is important, it is not sufficient to address the growing threat.

In order to properly secure Wireless Local Area Networks (WLANs) techniques to directly address the threat must be applied to the environment. This paper outlines the techniques used to monitor WLANs and provides evaluation criteria for selecting an appropriate solution for all WLAN deployments.

About Spire Security

Spire Security, LLC conducts market research and analysis of information security issues and requirements. Spire provides clarity and practical security advice based on its “Four Disciplines of Security Management,” an operational security model that encompasses identity management, trust management, threat management, and vulnerability management. Spire’s objective is to help define and refine enterprise security strategies by determining the best way to deploy policies, people, process, and platforms in support of an enterprise security management solution.

This white paper was commissioned by AirDefense. Spire Security maintains its independence regarding the content and assertions that is the product of years of security audit, design, and consulting work.



Selecting a WLAN Monitoring Solution

Table of Contents

INTRODUCTION	1
Four Disciplines of Security Management	1
VALUE OF WIRELESS MONITORING	1
SELECTION CRITERIA FOR WLAN MONITORING	3
Architecture	3
Wired-Side Monitoring	3
Roaming Sniffer Monitoring.....	3
Native Access Point-Based Monitoring	3
Dedicated Sensor/Manager solution	4
WLAN Monitoring Feature Set	4
Capture/Monitor	5
Discover	5
Analysis/Correlation	6
Response.....	6
Forensics	7
Enterprise Readiness	7
SPIRE VIEWPOINT	8



Introduction

Information technology executives are quickly recognizing that wireless LANs (WLANs) have become a mainstay in corporate environments and will increase in importance over time. The infrastructure requirements are minimal and wireless provides a flexible way to manage connectivity to client PCs and other portable devices. Along with this ubiquity comes the need to better control the infrastructure and secure WLANs.

The value in WLANs is their ability to cover a broad area without the need to pinpoint individual connection points. But this broad area often incorporates sensitive areas, like adjacent offices, parking lots, public areas, or other easily accessible places. In addition, the area can be extended by users with directional antennas. So the flexibility that allows the introduction of all sorts of devices also brings along baggage of making it easier to attack and disrupt the network's operations. WLAN security, therefore, is at the forefront of extending this infrastructure to accomplish the anticipated gains of WLANs.

Four Disciplines of Security Management

Security management encompasses four disciplines – four areas of focus for managing and protecting information systems to ensure security coverage for the enterprise or individual platforms. These four disciplines are:

- ▶ *Identity Management* focuses on how users gain and use their corresponding user accounts, and all activities in the issue/maintain/disable/delete account lifecycle.
- ▶ *Vulnerability Management* focuses on how systems and applications should be hardened to resist any type of attack. Emphasis is on the scan/detect/fix/mitigate vulnerability lifecycle.
- ▶ *Trust Management* focuses on strengthening the functional application at all layers by designing security into the architecture and encrypting data in transit and at rest.
- ▶ *Threat Management* focuses on monitoring all activity and discerning between malicious activity and legitimate activity.

Each of these disciplines can be applied to WLANs. Identity management integrates 802.1x and LEAP authentication for identity management. Layer 2 switches and access control devices provide vulnerability management. encryption and VPN devices secure the data in transit for trust management. And finally, wireless logging and monitoring capabilities provide threat management that complements the other three disciplines. Monitoring ensures that all users are properly authenticated and all traffic is properly encrypted while identifying new network vulnerabilities. The rest of this paper is focused on monitoring wireless environments for security and management control purposes.

Value of Wireless Monitoring

No matter how much attention is paid to security during the design phase of an implementation, the value of monitoring becomes paramount to the success of the deployment. Often, project managers will begin the security discussion by identifying what type of authentication and encryption will be put into place for protection. While this is a good first step, it neglects to address the social engineering and system vulnerability aspects of security.



Selecting a WLAN Monitoring Solution

At some point, usually during the prototyping phase of a deployment, project managers also realize just how expensive (from a manual process and system processing perspective) authentication and encryption can be. This is the point where the value proposition for WLAN monitoring shows up clearly.

To be more specific, all WLAN deployments include inherent security exposures that can never be addressed through authentication and encryption alone. These characteristics include:

- ▶ **Device Attraction** – Like a lonely man in a crowded nightclub, the protocols used in WLANs are designed to constantly prowl for a connection/association with an access point or another WLAN device. Most new laptops are coming with built-in WLAN support, and WLAN-enabled employee laptops are at risk of accidentally connecting to a neighboring company's access points.
- ▶ **Uncontrolled Medium** – Few enterprises can control their entire WLAN “footprint” or WLAN airspace that bleeds into uncontrolled areas, such as neighboring offices and open public areas, where intruders can passively observe network traffic and capture authentication credentials or attempt to connect with the network. If insecurely connected to the wired network, an access point can leak critical network information, such as multicast and broadcast traffic into the airspace. This can provide information about wired network topology, protocols, and devices to intruders sniffing the airwaves who can then use this information for a “structured attack” that bypasses wired-side IDS.
- ▶ **Rogue WLANs** – With minimal equipment costs, WLANs can spring up anywhere and everywhere, regardless of any policy that might attempt to ban them. A quick trip to the local computer store and an Ethernet connection later, and a fully functioning WLAN is born. However, rogue WLANs are more than unauthorized access points. Soft APs – laptops running software to act as an access point – are easy to set up and hard to detect. WLAN-ready Windows XP laptops are widely used. By default, they probe for connecting to access points and are a probably a bigger security risk than rogue access points.
- ▶ **Ad hoc Networking** – WLAN devices support peer-to-peer, ad hoc networking, that can expose an enterprise laptops to malicious associations. In ad hoc networking, two laptops can connect with each other without requiring an access point. In new laptops, wireless capability comes as part of the standard configuration with no form of encryption or authentication.

With the ease in which WLANs can appear, enterprises must recognize that any insecure WLAN can create a backdoor to the network that circumvents wired-side security. Monitoring helps in the following ways:

- ▶ Identifies rogue WLAN devices that crop up everywhere, by design and by mistake. Nowadays, these devices may be access points, client PCs (desktops/laptops), PDAs, and other special-purpose devices, such as printers and barcode scanners.
- ▶ Detect network critical information (multicast, broadcast traffic) that may be leaking into your airspace. Once you understand what is leaking and where it is leaking, steps can be taken to put in place gateways and lock down access point configuration to stop it.
- ▶ Enables policy enforcement by detecting violations and ensuring that WLAN deployments and use are sanctioned by the organization in a controlled manner. Monitoring for policy ensures that the security designed in the WLAN is not bypassed.
- ▶ Detects network scans and attacks against any of the WLAN infrastructure, particularly if these

attacks can penetrate inside the network perimeter (as is typical) or occur in a public place (like airports, hotels, or retail stores).

- ▶ Provides management-critical intelligence for identifying device failures, troubleshooting performance issues, and understanding traffic patterns and network utilization.

Selection Criteria for WLAN Monitoring

Every organization should be evaluating how to monitor their WLAN environments – both sanctioned and potential rogues. This section describes the characteristics that should be evaluated to gain comprehensive monitoring coverage in an environment. There are three key areas to this evaluation: architecture, feature set, and enterprise-readiness.

Architecture

The first step in protecting WLANs is determining the type of architecture that a solution may use to address the problem.

Wired-Side Monitoring

A completely wired solution attempts to manage WLAN threats in the same way as the wired threat. These solutions scan for protocol patterns that are indicators of WLANs, monitor layer 2 activity to identify roaming MAC addresses, and generally use existing knowledge of the infrastructure to deduce where and how wireless LANs are in use in the environment.

The strengths of a solution like this are apparent – they are fairly simple to deploy and manage, and therefore tend to minimize the total cost of ownership of the infrastructure. In addition, they often integrate into more comprehensive monitoring and scanning solutions, and may deploy as a service. On the down-side, wired-side solutions cannot recognize WLAN traffic in the air. Therefore, it cannot detect Soft APs, probing laptops, accidental association, or ad hoc networking between laptops. Nor can they recognize rogue access points with spoofed MAC addresses, ad hoc networking between laptops, policy violations among WLAN devices, and attacks against the WLAN.

Roaming Scanner/Sniffer Monitoring

A WLAN scanner works by probing access points to collect basic information about them. A WLAN sniffer works in wireless airspace and passively observes WLAN traffic to identify WLAN devices. Typically, these solutions are deployed on mobile laptops or PDAs, with or without directional antennas, and they seek out a signal within the detection range. The primary purpose of a scanner solution is to identify rogue access point. They can usually also identify some basic configuration issues such as default SSIDs and whether encryption is enabled or not.

Getting started with wireless sniffers is very inexpensive and it provides a basic idea of the magnitude of the wireless security problem. It is often the first thing an enterprise does to evaluate the risk and can provide the justification necessary to implement a fuller solution. But manual site surveys with handheld or laptop tools have scaling issues. Generally, coverage is limited by the number of personnel assigned to the task, the physical (geographic) area that must be covered, and the frequency of the evaluations. They do little or no deep-content analysis to identify pervasive threats and don't provide WLAN aggregation and correlation analysis.

Native Access Point-Based Monitoring

A native access point solution embeds security capability into the access point. Embedded security in an AP should be an expectation for any enterprise. This security typically revolves around hardening

the system, or the vulnerability management capabilities, and uses authentication and encryption to harden the usage process. Enterprise WLAN systems are moving to include monitoring functionality from the access point infrastructure. The main benefit of this architecture is that it utilizes the same WLAN infrastructure for monitoring. This provides added insight to the authorized WLAN environment and keeps total cost of ownership down.

However, access point-based monitoring is limited to the coverage area of the access point; they cannot detect rogue access points in areas without an authorized WLAN. Other drawbacks of AP-based monitoring stem from the access point's standards support and settings. Access point-based monitoring may not be able to monitor WLAN devices and traffic on all 802.11 standards (802.11 a, 802.11b, and 802.11g), illegal channels, or channels other than for which it serves users. Finally, access points are subject to direct attack on availability (denial-of-service) and integrity (spoofed or modified information).

Dedicated Sensor/Manager solution

A distributed sensor and manager solution dedicated to monitoring creates a separate wireless "forcefield" around some physical area. While it retains a connection to the wired network, the wireless sensor is not a functional access point. It exists solely to identify malicious wireless activity, improperly configured WLAN devices, and WLAN operational issues. This purpose-built capability creates different architectural opportunities to protect a physical area.

Dedicated wireless monitoring solutions provide complete out-of-band control over the threat. This ensures broad coverage, particularly if the access point is the target of an attack. Given the distributed architecture, it also provides an opportunity to correlate data to monitor multiple attacks against access points or roaming systems. On the down side, it adds a layer of security management to the environment.

When evaluating a wireless LAN monitoring solution, an enterprise should balance the tradeoffs between the deployment costs of the dedicated sensor architecture versus the limitations of wired-side scanning, roaming sniffers, and AP-based systems.

WLAN sniffer and scanner vendors have moved to design their code to operate across independently running sensors that process all traffic locally and send alerts and summary stats to a central server. This paper should assist IT buyers understand the differences between distributed scanners and an enterprise WLAN monitoring solutions.

WLAN Monitoring Feature Set

The core features of a monitoring solution require full coverage in the threat management lifecycle. While capturing beacons and SSIDs from the air can be relatively easy, a comprehensive WLAN monitoring solution processes and correlates the information to provide actionable information. The functions include capture/monitor the data; provide discovery capability; conduct correlation and analysis; response; and forensics (Figure 1). For each of these lifecycle functions, WLAN monitoring solutions have features for evaluation.



Figure 1. WLAN Monitoring Functions

Capture/Monitor

In the first phase of the lifecycle, a wireless monitoring solution collects the packets. Pertinent questions include:

- ▶ What protocols does the solution decode? Any solution must be evaluated based on whether it supports layer 2 protocols including 802.11a, 802.11b, and 802.11g. An organization may standardize on 802.11a but will still need to monitor for any rogue devices for 802.11b and g.
- ▶ How does the solution maintain state? A solution should retain information about sessions and state in order to develop a contextual understanding of WLAN usage and the relationships between all connecting devices. Like a video camera compared to a photo camera, stateful monitoring powers the detection of certain intrusions that are otherwise missed.

Discover

The second phase involves basic discovery to automatically identify the WLAN infrastructure. Questions to ask:

- ▶ How does the solution detect rogue access points? Seeking out SSID broadcasts is the most common method but prone to missing APs that are being hidden and do not broadcast their existence.
- ▶ Can the solution discover WLAN laptops and other stations? Can it identify laptops that are probing and looking to connect with access points? Can it detect accidental associations? Can it detect ad hoc networks?
- ▶ How does the solution perform network mapping and inventory functions? Gaining insight into the WLAN assets allows for control of configurations and assets.
- ▶ How does the solution perform fingerprinting of devices and applications? One can gain a better understanding of risks and vulnerabilities with a full set of information about the resources in use.

Analysis/Correlation

The third phase is the intelligence phase. This is the point where full analysis of the packets and traffic is accomplished.

- ▶ Can the solution analyze the 'health' of a legitimate WLAN? Health monitoring provides insight into the proper use of a WLAN and alerts network managers to device failures and other operation issues, such as channel interference or an access point overloaded with too many connecting stations.
- ▶ Can the solution monitor for customized policy violations for configuration, security, and usage? Centralized policy management is a first-level requirement for correlation. A WLAN monitoring solution should monitor for defined policies, such as device configurations, performance thresholds, approved vendors, authorized devices, and approved channels.
- ▶ What intrusion detection techniques are in use? Techniques include basic signature and rule based detection; protocol anomaly detection; traffic anomaly detection. No single technique is sufficient to detect intrusions. These intrusion detection technologies should be correlated for accurate results and reduced false positives.
- ▶ Does the solution provide the ability to recognize roaming devices? An organization may allow certain WLAN laptops to roam among a set of access points in a department but may prohibit roaming and connecting to certain other access points.
- ▶ Can the solution aggregate and correlate data from multiple sensors and across time? Again, roaming means that understanding and comparing activity from multiple access points can provide new insight into the nature of the threat and specific attacks against the infrastructure. Multiple sensors may recognize the same access points and stations, and correlation eliminates duplicate alerts, correctly identifies spoofed devices, and provides an accurate picture of WLAN devices and their activity. Network correlation is a differentiating technology for enterprise-class WLAN monitoring systems.
- ▶ Does the solution provide central management of multiple sensors? At some point, with many sensors deployed, central management is a must to aggregate the activities and provide for configuration and administration control.

Response

The fourth phase incorporates response capabilities; the action taken when an alert is received or when sensors identify new information about a WLAN deployment.

- ▶ Can the solution send email and SMS notification alerts to various IT personnel based on the type of alert (security vs. management), location of the event, and the severity of the alarm?
- ▶ Can the solution integrate with traditional network managers or security consoles through SNMP or Syslog? SNMP integration allows alerts to be sent to SNMP managers such as IBM Tivoli, HP OpenView and NetCool.
- ▶ Can the solution reconfigure access points if they are found to be out of compliance with policy or generally weak? This general management requirement ensures that authorized access points remain configured with the performance needs and security standards of an organization.
- ▶ Can the solution terminate connections? When clearly malicious activity is identified, it is of

obvious value to be able to immediately terminate the connection of a station to an access point or an ad hoc network between two users.

Forensics

The final phase in the lifecycle is forensics – the ability to determine exactly what went wrong and work it to conclusion. Forensic analysis requires historical and detailed understanding of WLAN devices, their connections, and their behavior over time. Forensics activities can determine things like when a user station or access point came online, the length of time of connections, the stations connected to a compromised access point, and the type/extent of data being moved through the network. Pertinent capabilities include:

- ▶ Can the solution monitor standard control and management activities to provide detailed information about traffic? Network management involves traffic analysis and if monitoring is already occurring, then leveraging the investment is a valuable proposition.
- ▶ How does the solution contribute to incident management? Once an intrusion or problem is identified, it must be managed through to resolution. The ability to manage and track incidents becomes an important addition to a WLAN solution.
- ▶ Can the solution provide insight into root cause? Root cause analysis ensures that symptoms are addressed as part of the big picture.

Enterprise Readiness

All the features in the world don't matter if the solution doesn't meet the needs of the enterprise from an integration standpoint. This means the traditional capabilities must be considered:

- ▶ What are the deployment requirements? The extent of configuration and design requirements prior to deployment and the knowledge required to build the system are key ingredients that must be considered. For a deployable solution, many enterprises choose an appliance-based WLAN monitoring system that eliminates the need for time-consuming integration of hardware, database, and application software.
- ▶ What management and administration capabilities are offered? For the devices themselves, the ability to provide functional authorization to multiple administrators and the organization of the interface determine the ease with which the solution will be managed. Alerts generated for the headquarters location may need to be handled by one person but alerts for a manufacturing plant may need to be managed by another person. Most enterprises require role-based user accounts, centrally managed policy, automatic system updates, and centralized updates for sensor agents.
- ▶ What security features are built in the monitoring solution to protect itself? Can the sensor be hijacked to redirect WLAN traffic that it's observing? Can the sensor be brought down by DoS attacks from the air or from the wired side? Perhaps obvious for a security solution is the need to have the architecture hardened well to protect against direct attack. Securing the sensor, servers, and all communications are assumptions that must be verified. Enterprises should look for a hardened operating system, encrypted communication, and certificate-based authentication.
- ▶ How scalable is the solution? Particularly with WLANs, the expectation of wide deployment is common. A solution must be able to scale along with the enterprise's needs. Enterprises should consider the coverage area of a sensor agent, how many access points and devices a sensor can handle, and the capacity of each application or appliance.

- ▶ What are the performance capabilities of the solution? Meeting the needs for bandwidth and processing is an obvious requirement for any solution. A monitoring system must not overburden the existing wired infrastructure. A monitoring solution should also be reliable and provide redundant or failsafe capability.
- ▶ How reliable is the monitoring solution? Does it support high availability or primary/secondary fail-over configuration? A monitoring solution becomes a critical component itself and must be reliable in order to be relied on.

Spire Viewpoint

Within 2 years, wireless LANs will be a key component to everyone's wired LANs and will be deployed ubiquitously in public access environments like hotels, airports, and shopping malls. The area-based access enabled by wireless solution requires careful consideration of what activity is occurring on the network and what access is provided once allowed into some larger virtual entity, such as a LAN, WAN, or MAN. A comprehensive approach to WLAN monitoring is key to securing this shared environment to provide the enabling capabilities for ubiquitous computing while still protecting against attacks and misuse.

Contact Spire Security

To comment about this white paper or contact Spire Security, LLC about other security topics, please visit our website at www.spiresecurity.com.

This white paper was commissioned by AirDefense. Spire Security maintains its independence regarding the content and assertions that is the product of years of security audit, design, and consulting work.