

The Hidden Threat: Misconfigured Access Points



In the IT industry, a great deal of attention is focused on the threat of unauthorized, or "rogue," access points. Surprisingly little attention is paid to a significantly more serious threat to WLAN security: the misconfigured AP. Centralized management solutions like the AirWave Management Platform™ offer the best defense.

Enterprise-class wireless access points in large corporations and other organizations have dozens of configurable settings related to security:

- What encryption settings will be used to protect wireless data (WPA, WEP, none)?
- Should the access point broadcast its name publicly?
- Should access be restricted to a predefined list of devices?
- Which access control server will tell the AP whether specific users should be allowed to connect to the wireless network?
- Will different classes of users be segregated onto different VLANs?

"Through 2006, 70% of successful WLAN attacks will occur because of misconfigured access points or client software."

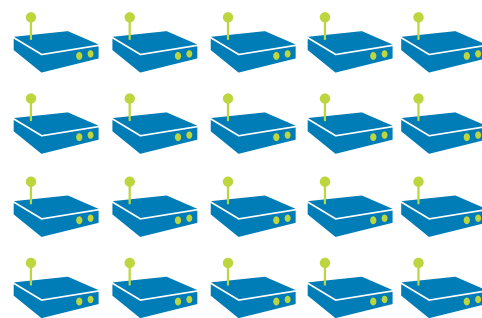
*Gartner Group,
August 2004*

If any one of these critical security settings is improperly configured at any of your access points, your entire network could be open and vulnerable to attack. An improperly configured access point represents an even greater threat than a typical rogue AP, because the misconfigured AP is difficult to detect via manual processes. Locating a misconfigured AP is truly like searching for a needle in a haystack. Because that AP is authorized as a legitimate device on your network, it will not trigger alerts in most intrusion-detection systems. As long as the AP continues to function, neither users nor administrators are likely to discover that security has been compromised. Misconfigured APs and the vulnerabilities they cause often go undetected for weeks or months.

The risk posed by access point misconfiguration is extraordinarily high, both because the error is so common and because many organizations fail to take proper steps to eliminate the danger. In effect, these organizations simply gamble that all of their access points are properly configured. As their Wi-Fi networks expand to more locations and more devices, this becomes an increasingly risky assumption.

Potential Causes of Access Point Misconfiguration

- Ambiguous or poorly communicated AP configuration policies
- Configuration errors made during installation, when installers are not security experts or when multiple installers are employed in diverse locations
- Human errors made by IT staff when troubleshooting WLAN problems
- APs that default to factory configurations when rebooted or upgraded
- Security policy changes that are not uniformly implemented across the entire infrastructure (e.g., shift from WPA to WPA2)
- APs that are relocated to network segments with different security policies
- Malicious intruders who disable security settings to access your network



Which AP is misconfigured?



If you cannot manage your network, your network cannot be secure.

The only way to guarantee the security of your WLAN as it grows into a mission-critical network is to implement a centralized solution such as the AirWave Management Platform™ to automatically configure and audit your Wi-Fi infrastructure. To protect your wireless network, the AirWave Management Platform allows you to:

Automatically locate wireless access points anywhere on your network.

The first step toward eliminating the threat of access point misconfiguration is to discover every wireless AP on your network, regardless of the makes and models of your access points and switches. The AirWave Management Platform uses a variety of standard (e.g., HTTP, SNMP) and proprietary (e.g., CDP, OSU, WNMP) discovery protocols to automatically locate access points on your network and download their current configuration.

Define security policies in a centralized fashion.

Once all access points have been discovered, AP configuration policies must be defined clearly and centrally to ensure that they are consistently applied across the entire network. While policies must be defined and enforced centrally, you will need the flexibility to specify different policies for different network locations (i.e., corporate training center vs. secure R&D facility). With the AirWave Management Platform, you can efficiently define specific configuration and security policies for multiple groups of access points on your network.

Automatically configure access points anywhere on the network.

Once policies are defined, they must be successfully applied to each access point on the network. On any network with multiple APs, manual configuration takes an inordinate amount of time and introduces great potential for human error. The AirWave Management Platform configures each AP automatically according to your policies, and then verifies that configuration and security settings have been correctly applied. This autoconfiguration capability enables you to quickly and accurately implement changes to security policies and other settings across your entire WLAN.

Continuously audit and automatically repair access point configurations.

It is not enough to ensure that an access point is configured with the appropriate security settings when it is first installed. To maintain WLAN security, frequent and automatic auditing of AP configurations is essential. Because manual audits are both impractical and expensive, an automated, centralized configuration auditing capability is critical to maintaining network security. When the configuration of an AP does not comply with your policies, the AirWave Management Platform notifies you of the potential network security vulnerability and attempts to automatically repair the misconfiguration by restoring the appropriate settings.

VARIABLE SETTING	ACTUAL CONFIGURATION	POLICY
SSID	Sales	Sales
Encryption	None	WPA Required
Open Network	Yes	No
Channel	6	6

