Untitled Document

Enterprise Approaches to Detecting Rogue Wireless LANs

Enterprises that delay in deploying 802.11 wireless LANs are facing increasing risks of employees installing their own rogue wireless LANs to the enterprise network. Driven by the desire for mobility and fueled by the decreasing prices of wireless LAN hardware, these employees circumvent an enterprise's investment in IT security by plugging a $60 wireless LAN access point into an Ethernet jack and connecting a $50 wireless access card to a station.

These rogue wireless LANs are easy to install and provide the mobility that employees seek. However, the end result is a wide-open entry point to the greater enterprise network. A rogue wireless LAN effectively extends an Ethernet connection to anyone inside and outside the building. Enterprises that have decided not to deploy wireless LANs must first set a policy banning employees from installing their own networks and then determine how to enforce that policy.

This article introduces five approaches to detecting rogue wireless LANs and outlines the functionality and limitations of each.

In confronting the issue of rogue wireless LAN detection, IT security managers should evaluate various approaches based upon technical requirements, enterprise scalability, cost, and ability to cover the future needs of network security.

1.) Wired-side Intrusion Detection System
A wired-side intrusion detection system (IDS) offers absolutely zero ability to detect rogue wireless LANs but can be useful in a limited capacity. While intruders entering the network through a rogue wireless LAN appear mostly as authorized users, a wired-side IDS may alert IT security managers when the intruder tests wired-side security measures.

A wired-side IDS fails as an effective approach to detecting rogue wireless LANs because it cannot identify:

2.) Wired-side SNMP Polling
Simple Network Management Protocol (SNMP) polling can be used to query information from IP devices attached to the wired network, such as routers, stations, and authorized access points. This process requires that the IT security manager conducting the SNMP poll to know the IP address of all devices being polled, which must also be configured to enable SNMP. For these reasons, SNMP polling is not an effective approach to detecting rogue wireless LANs. The IT security manager is not likely to know the IP address of the rogue access point, and the rogue access point is not likely to have SNMP enabled.

In addition, an SNMP poll against an authorized station operating as a Soft AP would not detect any wireless LAN activity. SNMP polling also would not detect accidental associations or ad hoc networking between stations.

3.) Wired-side Network Scanners
Wired-side network scanners work similar to SNMP polling to identify IP devices attached the network and key characteristics of those devices, such as MAC addresses and open ports. Rather than the SNMP protocol, scanners typically use TCP fingerprints to identify various types of devices.

Most scanners employ Nmap ("Network Mapper"), an open source utility for network exploration and security auditing. Nmap allows a scanner to quickly identify a large number of devices on a network by sending specially crafted TCP packets to the device. The response from each device is then compared to a set of known TCP fingerprints. Nmap-TCP fingerprinting can identify rogue access points attached to the wired network with some success. However, in some tests it incorrectly identified a Cisco Aironet access point as a SonicWall firewall.

Network scans can also be extremely intrusive while they require that an IT security manager have access to all the IP devices on the network and know all IP addresses. To locate every rogue access

point, a scan would have to be performed on the entire network, which would cause personal firewall alerts and multiple alarms from network intrusion detection systems.

Wired-side scanning can be centrally managed for a large enterprise but does not work well across subnets unless the network is configured with proper authorizations for polling requests to go across different routers. This may require reconfiguring various routers while causing extra effort and additional security risks. For this reason, wired-side scanning does not scale to support the needs of larger enterprises.

Using TCP fingerprinting, a network scanner cannot distinguish a rogue access point from an authorized access point but would rely on an IT security manager to sort through the results to determine rogue and sanctioned access points.

Wired-side network scanners are not an effective solution for enterprise rogue wireless LAN detection because wired-side scanners:

4.) Wireless Scanners & Sniffers
Wireless sniffers and scanners differ greatly from wired-side tools because wireless sniffers and scanners capture and analyze wireless LAN packets from the air. By monitoring the airwaves for wireless LAN activity in the area, wireless sniffers and scanners detect most access points and active wireless stations within range. They also can provide detailed information about the configuration and security employed by each device.

Design engineers and network administrators typically use freeware and commercial sniffers, such as Ethereal, AiroPeek, and Network Associates' Sniffer Wireless, to diagnose and trouble shoot network problems by analyzing wireless LAN traffic. However, sniffers provide granular information about the "sniffed" wireless LAN packets, which often require expert 802.11 security analysts to read the data and understand the threats detected. Freeware and commercial scanners, such as Netstumbler and AirMagnet, survey the airwaves for wireless LAN activity and requires a network administrator to sorts through the access points detected to determine which are unauthorized.

Both sniffers and scanners are limited by their need for a network administrator to physically walk the area with a laptop or hand-held device running the sniffer or scanner application. A September 2002 research brief from META Group questioned the viability of wireless sniffers and scanners for enterprise security.

> *Current radio frequency scanning tools such as Sniffer Wireless and AirMagnet are limited in their ability to perform scalable and repeatable audits.*
>
> *- **META Group, September 2002***

While this process requires the physical presence and valuable time of a network manager, the effectiveness is limited because it only samples the airwaves for threats. New rogue access points and other vulnerabilities can arise after a scan and will not be detected until the next time a network administrator surveys the network.

This approach is particularly unreasonable for enterprises operating dozens of offices around the country or retailers with hundreds of stores. Even if these organizations could feasibly devote a network administrator's full attention to survey each site on a monthly basis, rogue access points and other vulnerabilities can pop up the minute the survey is completed.

Because freeware scanners and sniffers are commonly available and commercial products are often priced under $5,000, many enterprises begin their rogue wireless LAN detection with these applications. Smaller organizations operating in a single location without potential for growth may find sniffers and scanners to be their most cost-effective solution if the organization is willing to accept the threat of rogue wireless LANs popping up between network audits.

The vast limitations of physical site surveys and the demands for personnel time limit the effectiveness of sniffers and scanners for large enterprises. Sniffers and scanners are simply not cost-effective for an enterprise with multiple locations or sensitive information that cannot risk rogue networks operating between security audits. In addition, IT security administrators would find this decentralized approach extremely difficult to manage and collect information for multiple locations.

	Wired-side IDS	Wired-side SNMP	Wired-side Polling	Wireless Scanners & Sniffers	Centralized management with wireless sensors
Technical Requirements					
- Detect Rogue APs	No	Limited	Limited	Limited	Yes
- Detect laptop APs	No	No	No	Limited	Yes
- Detect ad hoc networks	No	No	No	No	Yes
Scalable for enterprise	No	No	No	No	Yes
Support future security needs	No	No	No	No	Yes
Total cost of ownership	No	Yes	Yes	No	Yes

5.) 24x7 Monitoring & Centralized Management for Enterprise Rogue Detection - AirDefense RogueWatch
Enterprise rogue wireless LAN detection requires a scalable solution that combines the centralized management of wired-side scanners and radio frequency analysis of wireless scanners. RogueWatch from AirDefense provides this comprehensive solution with an innovative approach to wireless LAN security that includes a distributed architecture of remote sensors to monitor the airwaves for all wireless LAN activity and report to a centrally managed server appliance.

The remote sensors are equivalent to wireless scanners but add 24x7 monitoring to provide 100 percent coverage against rogue wireless LANs the minute they are connected to the network or enter the coverage area. The coverage area of the sensor varies upon the topology of the physical area, but a sensor typically provides a coverage area of nearly 1000 feet in all directions in most office buildings. All wireless LAN activity, including rogue access points, accidental associations, ad hoc networks, and Soft APs, are detected and reported to the backend server, which alerts IT security managers with an email or page.

The server appliance provides centralized management for rogue wireless LAN detection with a dashboard view of all wireless LAN activity, customized alarms based on severity of the security breach, hierarchical reports, and integration with other network administration tools, such as HP OpenView, Tivoli, and NetCool. All sensors are remotely managed from the central server over a secure HTTP connection.

This approach to rogue wireless LAN detection is akin to the security of physical buildings whereby video cameras are deployed at key locations for 24x7 monitoring and a central security station analyzes the incoming video for security risks. The video cameras reduce the need for costly security guards to walk through the building just as the remote sensors of RogueWatch replace the need for wireless scanners.

RogueWatch's enterprise approach to wireless LAN rogue detection satisfies all technical requirements by detecting all wireless LAN activity, including:

The centralized management and 24x7 monitoring of the airwaves provides a scalable and cost-effective solution that enables enterprise wireless LAN detection throughout multiple locations of an organization. One or two sensors are deployed in each location to provide comprehensive, 24x7 detection of rogue wireless LANs.

As new offices are opened, RogueWatch easily scales to secure that office with the addition of a sensor deployed in the new location. Once an organization deploys an enterprise wireless LAN, RogueWatch continues to monitor the network 24x7 for rogue access points and can be upgraded to

provide a comprehensive network security. The distributed architecture of RogueWatch supports an advanced wireless LAN intrusion detection and protection system.