Wireless LAN Security - March 30 2002

The purpose of this document is to share possible steps to securing your WLAN. These are options, some are easier to implement than others and not all will be available to you. Pick and choose; use them all, it is your choice. I use Cisco AP's and frequently refer to them in examples; they are not the only access points (AP) with all of these features. The goal is to make your WLAN undesirable to the casual attacker and difficult to penetrate for the determined attacker.

WEP

First and probably easiest to deploy is WEP, which stands for Wired Equivalent Privacy. That means it is designed to give you as much privacy as a wired LAN. It says nothing about security, the only thing it does is slow down potential attackers. There are arguments that it doesn't even provide equivalent privacy. I won't go into that here. Why use it then? Well, the majority of attackers are people poking around. They don't have the hour or more it would take to crack WEP, let alone the patience to do it. If there are two WLAN's in the area and one has WEP and the other doesn't, which do you think is going to be attacked first? Attackers want the easy prey, WEP is work. Some cards only support 40-bit, and some support 40 and 128-bit. I suggest using the highest your hardware can handle. I have yet to notice a slowdown because of WEP.

SSID

Changing your SSID from the default is a good idea. The reality is, it doesn't matter. Most AP's broadcast their SSID and programs like netstumbler can grab those broadcasts. Cisco AP's have the ability to disable SSID broadcasts, while this hides the SSID from netstumbler, other programs like AiroPeek can still grab packets and see the SSID. Changing from the default keeps other users in the area with the default SSID on their equipment from getting on your network by accident.

Power

A common measure used to prevent attack is turning the power down on the AP. By turning the power down, the range of the AP signal is reduced. While this might stop the casual attacker, it won't stop a determined one. An attacker can boost his own signal and use an antenna to connect to the lower power AP.

DHCP

Dynamic Host Configuration Protocol assigns IP's to any client that requests them. If you assign IP's statically, then you make more work for the attacker. He now has to determine the IP range for your network and assign himself an IP. Changing from the default range is suggested.

Authentication

Many AP products have the ability to authenticate via RADIUS or similar service. This is useful for controlling who can use the AP by maintaining a user list on a server. This can also be integrated into popular products like Active Directory and LDAP. The problem is that you may not be able to control attackers sniffing the wireless network. The packets are still vulnerable to capture.

MAC filtering

Another AP feature is MAC Address filtering. Cisco AP's have the ability to store list of allowed MAC addresses. This prevents other network cards from using the AP. This too isn't foolproof, as MAC addresses can be changed and spoofed. The catch is the attacker would need to know a valid MAC before he could use the network. Cisco AP's can also propagate this list to other AP's allowing you to manage one list.

Location

Place your AP outside the firewall or on a separate DMZ. This allows you to control access to resources behind the firewall.

Network Monitoring

Monitoring the network for attacks and strange behavior is handy. An IDS can fill this role well. Monitoring is not a security measure; it is more of a way to alert you to improper use.

VPN

This is the only real way to secure your traffic. While some VPN's are better than others, any VPN is better than nothing. A simple Microsoft PPTP server on the network can help encrypt all the traffic over the wireless LAN. IPSEC is an even better choice, but has issues with Network Address Translation (NAT). NAT is commonly used on consumer AP's and corporate networks. FreesWAN is a good choice for Linux environments; it has a bit of a learning curve, but works well. SSH can also be used to tunnel traffic.

Summary

Wireless LANs are not secure. In your deployment plan, include several of the above measures to help prevent attack. It will only be a matter of time before VPN features are included in AP's to help secure traffic over the air. Until then, you need to supply security measures yourself.

Jason Lewis
http://www.packetnexus.com