

Wi-Fi Security Measures and Vulnerabilities

SSID

SSID is Service Set Identifier, which differentiates one WLAN from another. Some people believe that the SSID works like a password, however it actually serves as a network identifier. Turning off SSID beacons only turns off the broadcasting of the identifier and only hides it from those not using a packet sniffer.

MAC Address Filtering

A MAC address is a unique address associated with every network device. Filtering basically allows only "known" devices to connect to the network, a similar concept to firewall rules. However, MAC Addresses can be sniffed with any packet sniffer. All a bad guy has to do is sniff traffic as each active connection contains the MAC Address information of the source and destination system. Any single packet can provide the MAC address. Once an unfiltered address is located the attacker can change his own MAC address by using a Windows based tool like SMAC, MACShift, or a-Mac, or a standard command line tool in UNIX.

WEP Encryption

WEP is Wired Equivalent Privacy and is based on the RC4 stream cipher used to encrypt wireless communications. Due to flaws in this approach, an attacker who can gather enough packets can crack the encryption. This used to take a long time to gather all the packets, however due to tools such as Aireplay; the attacker can trick the access point into providing packets at a much faster rate. For example, a 64 bit WEP key can be cracked in less than 10 minutes using openly available tools. It is also possible to perform dictionary attacks on WEP as users typically use a word that is easy to remember.

WPA/WPA2 Encryption

Wi-Fi Protected Access (WPA/WPA2), are stronger encryption schemes and are being used to replace WEP; however, they rely on a shared secret, usually a password. Any time a user provides a password, the chances of a dictionary attack become an issue. An average dictionary attack can try 30-60 words per minute. Most wireless access points do not log authentication attempts or lock users out for failed attempts so this attack can go undetected.