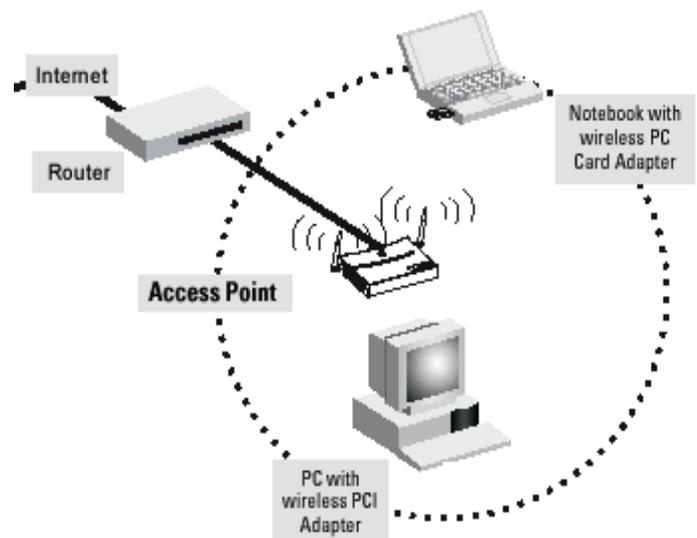


Wireless [In]security

We are often asked about the current state of security of a wireless network. This brief article highlights some of the security features on common wireless networks as well as ways that an attacker can circumvent that security and attempt to breach your network.

Encryption

There are two affordable and common types of encryption on the market today for wireless devices: WEP (Wireless Equivalent Privacy) and WPA (Wi-Fi Protected Access). Both wireless technologies have the ability to encrypt data up to a 128-bit cipher, but it should be noted that not all devices use this “strong” encryption level by default. In both cases (although approximately twice as long in the case of the WPA encryption), an attacker can “sniff” and collect enough packets of a certain type (called “Weak IVs”) from your wireless network in order to begin “cracking” your WEP encryption code. Packet Re-injection techniques can help an attacker generate large amounts of wireless traffic on your network in order to increase the number of Weak IV packets that are being sent (which need to be collected in large quantities in order to “crack” the code).



SSID (Service Set Identifier) Broadcast

Most wireless devices now have the ability to disable the clear text broadcasting of its wireless name (or its SSID – Service Set Identifier). The ability to disable this broadcast was initially designed as a security measure against wireless attacks. It was thought that, by disabling the access points sending the SSID, attackers would simply not be able to “see” the wireless network when sniffing. While the disabling of this SSID is a good recommended practice, those connecting to the access point still transmit the SSID in clear text during their handshake with the network. This makes it relatively easy for an attacker to identify this SSID.

MAC (Media Access Control) Address Filtering

Another security measure on most access points today is the ability to input a list of computer hardware addresses (called Media Access Control Addresses or MAC for short). The wireless access point will then only accept traffic from workstations or devices that have a MAC address within their list of authorized devices. While a recommended practice and an additional control, those authenticating to a wireless access point send their MAC address in clear text, again making it very easy to be “sniffed” by an attacker. Once “sniffed,” MAC addresses on an attacker’s machine can be “spoofed” or duplicated, circumventing this type of security.

Other Security Controls

Other security controls, such as directional antennas or tunneling protocols, are also available, along with more complex encryption options. Attackers are also becoming smarter. They can attack your wireless network and establish a connection without cracking encryption. Attackers do not have to follow the same FCC regulations that legitimate institutions must. By “boosting” the strength on their antennas and choosing the same SSID as your institution, an attacker can actually “bump” your clients off a wireless access point and have those clients connect to THEIR wireless access point. Thus they have made you connect to their network, and it is not even illegal for them to look at the machines that have connected back to their access point. In the end, this type of attack comes down to who has the stronger signal, and since attackers can use non-FCC-approved devices, they will almost always win that fight.

Wireless technologies, while convenient and helpful, are currently not as secure as their wired counterparts. Presently, many different types of attacks can compromise your wireless network. Worse, once on your internal wireless network, an attacker can attack the wired components of your network. At this time, Snodgrass recommends not using wireless technologies at your institutions. Should a strong business need exist for such a use, we recommend using some or all of the above-noted mitigating controls and keeping a close eye on which clients are connected to your wireless access points.

If your organization would like to learn more about wireless technologies and/or how we can help you test and secure this technology, please contact our Technology Services Practice (Andrew Olmo, Principal, or Jeremy Burris, Senior IT Audit Consultant) at 724-934-0344.