No. 111, October 2003

THE COMPUTER CORNER

No. 111. Wireless Networking

- by Richard Polivka, N6NKO

[This month we have a guest author. Richard (our Wisconsin ARES/RACES HF Net Manager), reminds us of a possible security hole that needs to be plugged. This is especially pertinent and important in this day and age, and becomes increasingly important as more of us are networking with wireless devices. Take a look, and remember Richard's words in the future if you set up a wireless network. Stan]

We have been told time and again to improve our security processes because of the undesirable changes in the world we live in. Everyone has to become more conscious of their surroundings and what is going on around them. Yet, one of the more innocuous items can escape our vigilance, and it can present some real grief in the end.

Probably the most active advance in communications right now is data transmission using the 802.11b networking protocols, more commonly known as "Wi-Fi". These wireless networking products allow computers to talk to networks without wires. Usually a company or an individual will have a Wireless Access Port (WAP) tied to their network with resulting access to the Internet. This is where the trouble starts.

Wired networks, by design, are quite secure since you must be physically wired to the network to use its facilities. Having a wireless port to the network opens up the possibility of anyone with the correct software and hardware to access your network and compromise the assets attached. Let me explain how this is done and how to protect your system from unwanted use and intrusion.

I have a laptop that has a wireless networking card installed in it. I use a freeware program that sends out ID packets, looking for responses, and it also just listens for broadcasts by other computers. The returned information is then displayed and recorded. The program displays the channel number, the SSID, manufacturer of the WAP, the MAC ID of the monitored WAP, whether or not the WAP is using Wireless Encryption Protocol (WEP), and the received signal strength. The breakdown is as follows: Channel Number is the channel that the WAP is listening to – there are 12 channels assigned to the US, the first six are in the 2.4 GHz amateur band and the rest are in the ISM band. The SSID is the identifier (station ID) of the WAP; and whether or not the Wireless Encryption Protocol (WEP) is being used.

I did a drive from my residence to my daughter's school and then into the office, a total of about 9-11 miles, with my laptop running the wireless networking card and the "sniffer" program. The results of my "war-driving" are as follows: 12 WAPs were located. Two were using encryption, six of them still had the factory default SSID in the port, only two channels were used out of twelve (Ch. 1 and Ch. 6), and two company's WAPs were unsecured. By knowing the SSID of the WAP and that it is unencrypted, I would just have to change the SSID of my laptop to the broadcasted SSID and viola! I will be using someone else's account for access, either for legitimate or illegitimate usage, if I was feeling a bit larcenous.

So, what does this have to do with security? An unsecured WAP is just begging for trouble to your ISP, your ISP account, your computers, and your network. How does one go about securing a WAP to minimize the possibility of intrusion? There are a few rules that need to be followed:

1) Change your SSID from the default setting
2) Turn off SSID broadcasting / identification (Loose lips sink ships)
3) Use 128 bit encryption
4) Change your encryption password on a weekly basis

5) Use a firewall program, such as ZoneAlarm Pro

Even with the SSID broadcasting turned off, if the WAP is in use by a remote PC, it can be seen. Be aware that the WEP encoding sequence has been cracked and that there are programs out there that can catch your packets and after receiving enough data (about 1 GB), can come up with the password and an intruder can get into your network. This is why I suggest changing your password on a short, regular basis. I change my WEP passphrase every week or sooner. If a WAP is being used at a company, it should not be interfaced directly to the building network. Since WEP encoding is so easily cracked, it would behoove the company from a network security point to have the WAP talk to a router that is configured to use Point-to-Point Tunneling Protocol (PPTP) for another level of network protection before accessing the building network.

With some common sense, 802.11b networking can be used to your advantage but it takes a little TLC to be safe and secure. Just remember the rules presented above and apply them religiously. Happy networking!