Three Reasons Not To Use Wired Equivalent Privacy

According to computerworld.com, WEP (Wired Equivalent Privacy) can leave your wireless network vulnerable to intrusions. Mathematicians showed that the RC4 key scheduling algorithm, which underlies the WEP protocol, was flawed from the beginning. While searching for flaws in the protocol, they first looked at the four million packets determined to be the required amount to crack a full router's password key. However, after further study, this figure was found to be a miscalculation. To have a 95% chance at cracking a full key, a more accurate number was calculated to be around eighty-thousand packets.

Reason One for not Using WEP

The WEP protocol can be cracked several different ways. The two most common ways are *packet injection* or *listening*. Packet injection sends ARP (Address Resolution Protocol) requests to the router. These packets are requests that prompt the devices on the network under attack to respond by sending pieces of the encryption back to the attacker's computer. The second way is virtually undetectable. If a device on one's network is sending and receiving information across a wireless access point, the attacker captures these packets and uses them to decipher the WEP key.

Reason Two for not Using WEP

The length of a password key is determined by its number of bits. The idea is that the more bits used to make a key, the more secure it makes a wireless network. This is a misleading fact. The length of the key only determines the amount of packets the attacker needs to crack it. A determined attacker is willing to wait the extra few minutes to crack the key.

Reason Three for not Using WEP

Shortly after WEP, a more advanced protocol was designed to better protect a wireless network. WPA (Wi-Fi Protected Access) is today's standard for securing wireless networks. WPA comes in two types, WPA-802.1x and WPA-PSK. WPA-802.1x is a good protocol to use for large businesses. This protocol version combines access point authentication with another layer of authentication through an external authentication service. This means that after the authenticating user associates with the wireless access point, his or her credentials are also checked against a locally stored database or external sources.

WPA-PSK (Pre-Shared Key), on the other hand, is a good version for small businesses and home use. WPA-PSK uses a similar method to WEP to generate the key, but in a more secure way. The user can use a pass phrase as the password which makes it harder for an attacker to crack the key. Attackers must have a word list containing your pass phrase to crack the encryption key. Even though such word lists are readily available online, using unique multiple words in a pass phrase can reduce an attacker's chance of cracking the key.

Conclusion

If one is using a Verizon or other common commercial router, for example, by default they are depending on WEP security. This could leave them vulnerable to being hacked not only for their access key but for all of their personal information. It is imperative that individuals and families take additional measures to secure their personal computers if they are connected to any network source such as the internet. The best method for the non-computer specialist is to contact a trusted technician to upgrade their security protocols to adequate levels while being able to explain their purpose and use.