Dec. 01, 2008

From the Dec. 2008 Issue

Recently, a letter was submitted to the editor asking about the security of wireless networks and how to secure them. In this month's column, we will examine wireless security and take a look at two emerging technologies, cellular data cards and WiMAX. All wireless devices have some type of security concerns depending on how they are configured and/or used. The various types of wireless connections provide different ways of connecting whether on the corporate network or the Internet.

Before jumping into the discussion of wireless devices, let's make sure the definitions and processes related to the topic are up to date.

WIRELESS OFFICE NETWORKS

Many accounting firms have considered wireless networking in their offices but remain concerned about security. We have all heard about WEP and the coverage in the media about how its encryption protocols have been compromised by hackers. While this is true and is a concern for wireless WEP-encrypted networks, WPA-protected networks do not have the same problem, provided a strong security key is utilized. A strong security key would be defined as a long string of characters generated at random from the 95 allowable keys. For instance, Maryhadalittlelambthatspent12daysinthepasture is a stronger encryption key than GTbh1256. It would take years to brute force attack the Mary phrase, but only a few hours to crack the GT phrase. If used properly, WPA can provide a secure wireless network connection for an accounting office. WEP should never be used because the encryption has been compromised.

Implementing WPA is a fairly simple process of configuring the device for

rely on the client or the free wired or wireless connections in the hotel for access back to the office to check e-mail, obtain files or perhaps work remotely through a terminal server. While the client network is hopefully secure, the hotel or other Wi-Fi hotspot is probably anything but secure. This opens our computers and our data to exposure to others who might want to examine the contents
of our computers. Using a software firewall helps block access to ports not being used, but there are many ports open on a computer that can allow someone to view information. Some of these ports may be opened by software, and we may have no idea that the ports are even open. For example, some HP printer software opens ports on the computer that allow for wired network connections to be established
with the computer. Hotel networks are rarely secured with any type of encryption. This allows users to access the hotel's network without difficulty. This very openness of hotel networks is what causes issues for many business travelers even if a VPN might be used.

Cellular data cards provide a better level of security and connection to the Internet and corporate network resources than connecting through the unsecured Wi-Fi network o fthe hotel or local cofee shop. The cards are installed on the laptop and connect the laptop directly to the Internet via the provider's network. While you have a direct connection to the Internet, the ability for others to see you on the cellular network is more limited than it is on a hotel or coffee shop network. This does NOT mean that the connection is secure. All it means is that you have eliminated the middleman in the connection. You are connected directly to the Internet via the cellular service in the same way your DSL or cable modem connects. Irrespective of the type of connection being used, a software firewall should be running on your workstation to protect against threats on the Internet.

THE FUTURE

client of Wi-Fi network, the cellular data connection can be quickly established and enable employees to work faster.

WiMAX is an emerging technology and is actually being adopted in the third world faster than it is in the United States because an existing infrastructure does not exist in the third world. Pakistan is currently the leader in adoption of WiMAX technology with 17 cities currently using the system and plans to get it set up in all 71 cities in Pakistan. It will come here in the United States eventually as our existing copper-based wired network ages and needs to have significant replacements. WiMAX is the future, and cellular is the bridge technology.

Definitions & Processes

Access Point (AP) – The central control point to which other wireless devices such as computers and printers authenticate to gain access to the corporate network.

Wired Equivalent Privacy (WEP) – This protocol was introduced in 1997 to secure wireless communication between devices and access points by encrypting the broadcast traffic. The protocol has been replaced by other protocols because its encryption algorithms have been compromised. Unfortunately, even with the protocol being compromised, it is still in widespread use today.

Wi-Fi Protected Access (WPA and WPA2) – These protocols were released as interim standards while the IEEE, the Internet standard setting body, worked on fixing the WEP protocol standard. This protocol has remained, been expanded and is becoming the standard for wireless encryption between the device and the access point. All wireless devices sold since September 2003 with the designation Wi-Fi Certified support this standard. This standard does have some interoperability issues with some devices, and as a result not all

equipment will work with WPA encryption, especially older equipment built before

the recent upgrade to the 3G standard has made this type of access much more stable and beneficial. Most of these cards run at a speed equivalent to a DSL connection.

Worldwide Interoperability for Microwave Access (WiMAX) –
This protocol provides wireless transmission of data using a variety of transmission modes such as point-to-point or cellular-like access. Speeds are much higher than other types of access such as Cellular or standard wireless. WiMAX is not currently a heavily adopted technology in the United States. Some believe it will replace other connection technologies in the future because of its higher speeds, cellular-like access, and because it can serve as a last mile connection to people currently underserved by other technology in rural or remote areas. It is a competitor to DSL and cable.

Virtual Private Network (VPN) – This is generally a software package that creates an encrypted connection, commonly called a tunnel, through the Internet to the office network from wherever the remote computer is located and connected to the Internet. This encrypted connection passes data from the remote computer to the corporate network without using the open and more public Internet to transmit the communication. The remote computer acts as if it is directly connected to the corporate network even if it is located hundreds of miles away and connected via a non-corporate controlled connection, such as cellular or a Wi-Fi hotspot.

CPA Practice Advisor is registered with the National Association of State Boards of Accountancy