Using Wireless Technology Securely

US-CERT

In recent years, wireless networking has become more available, affordable, and easy to use. Home users are adopting wireless technology in great numbers. On-the-go laptop users often find free wireless connections in places like coffee shops and airports.

If you're using wireless technology, or considering making the move to wireless, you should know about the security threats you may encounter. This paper highlights those threats, and explains what you need to know to use wireless safely, both in the home and in public. You will find definitions of underlined terms in the glossary at the end of this paper.

Home Wireless Threats

By now, you should be aware of the need to secure traditional, wired internet connections.[*] If you're planning to move to a wireless connection in your home, take a moment to consider what you're doing: You're connecting a device to your DSL or cable modem that broadcasts your internet connection through the air over a radio signal to your computers. If traditional wired connections are prey to security problems, think of the security problems that arise when you open your internet connection to the airwaves. The following sections describe some of the threats to home wireless networks.

Piggybacking

If you fail to secure your wireless network, anyone with a wireless-enabled computer within range of your wireless access point can hop a free ride on the internet over your wireless connection. The typical indoor broadcast range of an access point is 150 – 300 feet. Outdoors, this range may extend as far as 1,000 feet. So, if your neighborhood is closely settled, or if you live in an apartment or condominium, failure to secure your wireless network could potentially open your internet connection to a surprising number of users. Doing so invites a number of problems:

- **Service violations**: You may exceed the number of connections permitted by your internet service provider.
- **Bandwidth shortages**: Users piggybacking on your internet connection might use up your bandwidth and slow your connection.
- **Abuse by malicious users**: Users piggybacking on your internet connection might engage in illegal activity that will be traced to you.

[*] For detailed information on securing wired home networks, see "Home Network Security" <http://www.us-cert.gov/reading_room/home-network-security/>.

- **Monitoring of your activity**: Malicious users may be able to monitor your internet activity and steal passwords and other sensitive information.
- **Direct attack on your computer**: Malicious users may be able to access files on your computer, install spyware and other malicious programs, or take control of your computer.

Wardriving

Wardriving is a specific kind of piggybacking. The broadcast range of a wireless access point can make internet connections possible outside your home, even as far away as your street. Savvy computer users know this, and some have made a hobby out of driving through cities and neighborhoods with a wireless-equipped computer—sometimes with a powerful antenna—searching for unsecured wireless networks. This practice is nicknamed "wardriving." Wardrivers often note the location of unsecured wireless networks and publish this information on web sites. Malicious individuals wardrive to find a connection they can use to perpetrate illegal online activity using your connection to mask their identities. They may also directly attack your computer, as noted in the "Piggybacking" section above.

Unauthorized Computer Access

An unsecured wireless network combined with unsecured file sharing can spell disaster. Under these conditions, a malicious user could access any directories and files you have allowed for sharing.

Protecting Home Wireless

While the security problems associated with wireless networking are serious, there are steps you can take to protect yourself. The following sections describe these steps.

Make Your Wireless Network Invisible

Wireless access points can announce their presence to wireless-enabled computers. This is referred to as "identifier broadcasting." In certain situations, identifier broadcasting is desirable. For instance, an internet cafe would want its customers to easily find its access point, so it would leave identifier broadcasting enabled.

However, you're the only one who needs to know you have a wireless network in your home. To make your network invisible to others, see your access point's user manual for instructions on disabling identifier broadcasting. (In Apple wireless networking, this is called "creating a closed network.")

While this kind of "security through obscurity" is never foolproof, it's a starting point for securing your wireless network.

Rename Your Wireless Network

Many wireless access point devices come with a default name. This name is referred to as the "service set identifier" (SSIS) or "extended service set identifier" (ESSID). The default names used by various manufacturers are widely known and can be used to gain unauthorized access to your network. When you rename your network, you should choose a name that won't be easily guessed by others.

Encrypt Your Network Traffic

Your wireless access point device should allow you to encrypt traffic passing between the device and your computers. By encrypting wireless traffic, you are converting it to a code that can only be understood by computers with the correct key to that code. For more about encryption, see the US-CERT Cyber Security Tip "Understanding Encryption," http://www.us-cert.gov/cas/tips/ST04-019.html.

Change Your Administrator Password

Your wireless access point device likely shipped with a default password. Default passwords for various manufacturers are widely known and can be used to gain unauthorized access to your network. Be sure to change your administrator password to one that is long, contains non-alphanumeric characters (such as #, $, and &), and does not contain personal information (such as your birth date). If your wireless access point does not have a default password, be sure to create one and use it to protect your device.

Use File Sharing with Caution

If you don't need to share directories and files over your network, you should disable file sharing on your computers. You may want to consider creating a dedicated directory for file sharing, and move or copy files to that directory for sharing. In addition, you should password protect anything you share, and use a password that is long, contains non-alphanumeric characters (such as #, $, and &), and does not contain personal information (such as your birth date). Never open an entire hard drive for file sharing.

Keep Your Access Point Software Patched and Up to Date

From time to time, the manufacturer of your wireless access point will release updates to the device software or patches to repair bugs. Be sure to check the manufacturer's web site regularly for any updates or patches for your device's software.

Check Your Internet Provider's Wireless Security Options

Your internet service provider may provide information about securing your home wireless network. Check the customer support area of your provider's web site or contact your provider's customer support group.

Public Wireless Threats

A wireless-enabled laptop can make you more productive outside your office or home, but it can also expose you to a number of security threats. The following sections describe some of the security threats you face when using a public access point.

Evil Twin Attacks

In an evil twin attack, the attacker gathers information about a public access point, then sets up his or her own system to impersonate the real access point. The attacker will use a broadcast signal stronger than the one generated by the real access point. Unsuspecting users will connect using the stronger, bogus signal. Because the victim is connecting to the internet through the attacker's system, it's easy for the attacker to use specialized tools to read any data the victim sends over the internet. This data may include credit card numbers, username and password combinations, addresses, and other personal information.

Wireless Sniffing

Many public access points are not secured, and the traffic they carry is not encrypted. This can put your sensitive communications or transactions at risk. Because your connection is being transmitted "in the clear," malicious users can use "sniffing" tools to obtain sensitive information such as passwords, bank account numbers, and credit card numbers.

Peer-to-Peer Connections

Many laptop computers, particularly those equipped with 802.11-type WiFi wireless networking cards, can create ad hoc networks if they are within range of one another. These networks enable computer-to-computer connections, a situation that creates security concerns you should be aware of. An attacker with a network card configured for ad hoc mode and using the same settings as your computer may gain unauthorized access to your sensitive files. You should note that many PCs ship from the manufacturer with wireless cards set to ad hoc mode by default.

Unauthorized Computer Access

As is the case with unsecured home wireless networks, an unsecured public wireless network combined with unsecured file sharing can spell disaster. Under these conditions, a malicious user could access any directories and files you have allowed for sharing.

Shoulder Surfing

In public wireless areas, the bad guys don't even need a computer to steal your sensitive information. The fact that you may be conducting personal business in a public space is opportunity enough for them. If close enough, they can simply glance over your shoulder as you type. Or, they could be peering through binoculars from an apartment window across the street. By simply watching you, they can steal all kinds of sensitive, personal information.

Safe Wireless Networking in Public Spaces

Accessing the internet via a public wireless access point involves serious security threats you should guard against. These threats are compounded by your inability to control the security setup of the wireless network. What's more, you're often in range of numerous wireless-enabled computers operated by people you don't know. The following sections describe steps you can take to protect yourself.

Watch What You Do Online

Because you're likely to have an unsecured, unencrypted network connection when you use a public wireless access point, be careful about what you do online—there's always the chance that another user on the network could be monitoring your activity. If you can't connect securely using a VPN (see "Connect Using a VPN" below), then consider avoiding

- online banking
- online shopping
- sending email
- typing passwords or credit card numbers

Connect Using a VPN

Many companies and organizations have a virtual private network (VPN). VPNs allow employees to connect securely to their network when away from the office. VPNs encrypt connections at the sending and receiving ends, and keep out traffic that is not properly encrypted. If a VPN is available to you, make sure you log onto it any time you need to use a public wireless access point.

Disable File Sharing

File sharing in public wireless spaces is even more dangerous than it is on your home wireless network. This is because you and your wireless-enabled laptop are likely to be even closer to other wireless computers operated by people you don't know. Also, many public wireless networks feature peer-to-peer networking in which other computers will attempt to connect directly to yours. To leave file shares open in this kind of environment is to invite risk. To prevent attackers from gaining access to your sensitive files, you should disable file sharing when connecting to a public wireless access point. Consult the help file for your operating system to learn how to disable file sharing.

Be Aware of Your Surroundings

When using a public wireless access point, you should be aware of what's going on around you. Are others using their computers in close proximity to you? Can others view your screen? Are you sitting near a window through which someone, using binoculars, could get a view of your screen? If any of these conditions exist, your sensitive data might be at risk. Consider whether it

is essential to connect to the internet. If an internet connection is not essential, disable wireless networking altogether. If you do need to connect, use caution and follow the steps noted above.

Summary

The following sections provide a quick summary of the steps you should take to secure your home wireless network and to use wireless technology safely in public spaces.

Home Wireless Security

When you use a wireless router or access point to create a home network, you trade wired connectivity for connectivity delivered via a radio signal. Unless you secure this signal, strangers can piggyback on your internet connection or, worse, monitor your online activity or access files on your hard drive. By taking the following actions, you can help secure your wireless home network against these threats.

- Change the default system ID of your wireless access point or router.
- Change the default password for your system.
- Turn off identifier broadcasting.
- Encrypt wireless communications. (WPA-based encryption offers better protection than WEP-based encryption.)
- Use your router's built-in firewall to restrict access to your network.
- Keep your wireless system patched and up to date.

Public Wireless Security

Accessing a wireless connection from a coffee shop or airport terminal may be convenient and even fun, but you should note that public access points (frequently called hot spots) are often insecure. The following are some steps you should consider taking before connecting to a public access point:

- Use a virtual private network (VPN) if possible.
- Avoid using passwords and providing personal information to web sites.
- Encrypt your files.
- Be aware of your surroundings.

References and Further Reading

Articles and Web Sites

Bowman, Barb. "WPA Wireless Security for Home Networks," Microsoft, <http://www.microsoft.com/windowsxp/using/networking/expert/bowman_03july28.mspx> (2003).

Brain, Marshall. “How WiFi Works,” How Stuff Works, <http://computer.howstuffworks.com/wireless-network.htm/printable>.

Collins, Hilton. “Critical Steps for Securing Wireless Networks and Devices.” Government Tecnology, < http://www.govtech.com/gt/406582> (2008).

Dolcourt, Jessica. “How to secure your wireless network.” cnet Australia, <http://www.cnet.com.au/wireless/0,239028844,240064146,00.htm> (2006).

Lee, Wei-Meng. “Securing AirPort Extreme Networks with WPA,” O’Reilly Network, <http://www.oreillynet.com/pub/a/wireless/2003/12/18/wap.html> (2003).

Lee, Wei-Meng. “Setting Up an 802.11b Home Wireless Network,” O’Reilly Network <http://www.oreillynet.com/lpt/a/3333> (2003).

McDowell, Mindi. “Understanding Encryption” (US-CERT Cyber Security Tip ST04-019), US-CERT, <http://www.us-cert.gov/cas/tips/ST04-019.html> (2004).

Vamosi, Robert. “Beware your evil twin (hot spot, that is),” CNET, <http://reviews.cnet.com/4520-3513_7-5630181-1.html> (2005).

“Wireless Life,” CNN.com <http://www.cnn.com/SPECIALS/2004/wireless/> (2004).

Books

Gast, Matthew. *802.11 Wireless Networks: The Definitive Guide, Second Edition.* Sebastapol, CA: O’Reilly & Associates, Inc., 2005

Potter, Bruce and Fleck, Bob. *802.11 Security*. Sebastopol, CA: O’Reilly & Associates, Inc, 2002.

Negrino, Tom and Smith, Dori. *Mac OS X Unwired.* Sebastopol, CA: O’Reilly & Associates, Inc, 2003.

Ross, John. The Book of Wireless: *A Painless Guide to Wi-Fi and Broadband Wireless, Second Edition*. San Francisco, CA: No Starch Press. 2008.

Weeks, Roger et al. *Linux Unwired*. Sebastopol, CA: O’Reilly & Associates, Inc, 2002.

Glossary

802.11	802.11 is a specification for wireless local area networks (WLANs) developed by the Institute of Electrical and Electronics Engineers (IEEE). There are several 802.11 specifications. These specifications describe how a wireless-enabled computer or device communicates with a base station or wireless access point and with other wireless-enabled computers or devices.
Access point	In a wireless local area network (WLAN), an access point is a station that transmits and receives data. An access point connects users to other users within the network and can also connect the WLAN to a wired network.
Ad hoc network	A local area network in which computers and network devices are in close proximity to others on the network. These devices are connected temporarily or for specific purposes.
DSL	DSL stands for digital subscriber line. This is a dedicated, high-bandwidth telecommunications line provided by a telecommunications or telephone company. DSL lines are capable of providing high-speed internet access, but are only available to subscribers who live within a designated distance of a telephone company central office.
Encryption	In internet technology, encryption is the transformation or encoding of information into a form that can only be understood by someone who has the correct "key" for decoding it. It is an important tool for securing network traffic.
Hotspot	A hotspot is a wireless network node that provides an internet connection. More and more hotspots are becoming available in public locations such as airports, coffee shops, and hotels.
Piggyback	Piggybacking refers to illicitly accessing the internet through an unsecured wireless network.
Router	A router is a device that processes traffic entering and exiting a network. It examines individual bits of network traffic, known as packets, and determines where to send the packet. Routers can attach to computers on a network (or other routers) using cables. Wireless routers perform the same job as wired routers, only they convert network traffic to a radio signal. Routers in a home network are most often connected to a broadband cable or DSL modem.

VPN	VPN stands for virtual private network. VPNs are a secure way to use the internet as an extension of a private network. They use encryption and a special internet protocol to create a “tunnel” through the internet from one point to another. This traffic cannot be accessed by those unable to connect to the VPN. Businesses frequently use VPNs to secure private network traffic moving between two geographically distinct offices, or between remote employees using laptops and the home office.
WEP	WEP stands for wired equivalent privacy, a security protocol designed to provide a wireless network with a level of security and privacy comparable to that of a wired LAN. In WEP, data moving between computers and access points is encrypted.
Wi-Fi	Wi-Fi is short for wireless fidelity. The term applies to wireless networks that employ 802.11-type security. An organization called the Wi-Fi Alliance coined the term. This organization tests wireless products work together and certifies those that pass as "Wi-Fi certified" (a registered trademark).
WPA	WPA stands for Wi-Fi protected access. Like WEP, WPA is a security protocol designed to provide a wireless network with security and privacy. WPA provides stronger data encryption and better user authentication than WEP.