Vol. 02, No. 12 / December 2003

Wireless Internet 101

Thinking about applying 'Wi-Fi' to your practice? Here's a quick primer on how to get connected.

John Luo, MD

Assistant professor of psychiatry UCLA Neuropsychiatric Institute and Hospital Los Angeles, CA

Wireless fidelity, or "Wi-Fi," is gaining popularity in the medical profession and elsewhere. Some medical professionals are using Wi-Fi's anytime, anywhere Internet connectivity to access electronic medical information during hospital rounds and to immediately enter demographic information when admitting patients.

WHAT IT IS-AND HOW IT WORKS

Wi-Fi is a certification given by the Wi-Fi Alliance, a nonprofit international trade organization that tests 802.11-based wireless Internet products. The "Wi-Fi Certified" logo signals to purchasers that the product has met rigorous interoperability testing requirements and is compatible with products from different vendors.

Today, the term "Wi-Fi" also commonly describes wireless Internet. Technically speaking, Wi-Fi is the use of radio technology to provide Ethernet connectivity in the unlicensed 2.4 and 5 GHz radio frequencies. By contrast, Internet access provided by wireless modems is based on technology used in cellular phones.

802.11 is the standard protocol ratified by the Institute of Electrical and Electronics Engineers. 802.11b is the most commonly used standard; 802.11a and 802.11g are other options (Table).

WHY WI-FI?

Wireless Internet access via the 802.11 protocol offers:

- freedom to surf the Internet in your office, back yard, or elsewhere
- the ability to avoid using unsightly wires to connect computers in a local area network (LAN)
- significantly faster access than wireless modems and higher connection speeds than are available via telephone lines or electrical outlets.

HITTING THE HOT SPOTS

Aside from office and home, Wi-Fi can be used at "hot spots"-public access points at cafes, restaurants, coffee shops, hotels, airports, downtown business districts, malls, and retail stores. Some retailers provide free access to attract business,[1] while others pay to partner with wireless Internet service providers such as T-Mobile[2] and Boingo.[3]

It helps to check online for hot spots before heading out (visit the T- Mobile or Boingo sites or try the Wi-Fi FreeSpot Directory or other Web site guide). Because most network connections are automatic, however, you can turn on your notebook computer anytime and find out in seconds if a wireless Internet service is available. An indication usually appears on the screen if you are connected to a wireless LAN with Windows XP or Mac OS X, but older operating systems may require additional software. A Wi-Fi signal does not guarantee Internet access because many Wi-Fi providers require the user to log in.

An alternative is to look for 'warchalking'-a series of sidewalk symbols that appear on your screen to indicate nearby wireless

access[4] (click here to view warchalking symbols). Warchalking has raised legal and moral issues, though to my knowledge this tracking method is seldom used.

GETTING STARTED

Several components are necessary for wireless Internet in the home or office. First, broadband Internet access via a cable modem, digital subscriber line (DSL), or satellite must be established. Connecting via a dial-up modem is another option, but its connection rate is too slow to be shared among several computers.

A wireless access point, which serves as the 'base station,' is then connected to the modem. Access points often are sold in combination with a built-in router, which delivers network information to the appropriate destination.

Each computer connecting to the access point must have a wireless network adapter. For desktop computers, this can either be a peripheral component interconnect (PCI) card or a Universal Serial Bus (USB) device. Many notebook computers come with a built-in wireless network adapter but can also use a PCI card or USB device.

Once these devices are installed, the wireless network must be set up so that each device can communicate. Most network setups are automatically established and require little user intervention; however, the user must decide which wireless channel to use and whether a security key is required.

SECURITY RISKS

Wireless network use poses one major drawback: lack of security.

All wireless LANs have built-in wired equivalent privacy security, which uses a security key to limit access. In 2001, researchers at the University of California at Berkeley discovered flaws in the encryption algorithm designed to protect wireless LANs.[5] Software has since been designed to exploit this flaw and identify the security key in the wireless traffic, rendering this level of security useless.[6]

In health care, this risk raises the issue of whether wireless networking is compliant with the Health Insurance Portability and Accountability Act (HIPAA). Medical Records Institute Executive Director C. Peter Waegeman n indicates that access via 802.11b is clearly not HIPAA-compliant[7] and that other standards such as 802.11a or 802.11g should be used. Most healthcare systems, however, continue to use 802.11b because it is widely available and economical.

MAKING YOUR NETWORK SECURE

Although the 802.11b standard is extremely insecure, several practical issues ameliorate the security risk. For one, finding the security key provides access to the wireless network but does not guarantee access to private information. Disabling shared access to network computers offers additional security but will eliminate the benefit of sharing information over a network.

Several hardware and software innovations aimed at increasing remote network security are scheduled to be launched in the coming weeks.[8] Until these products reach the mainstream, you can prevent unauthorized network access by:

- Choosing an access point that restricts media access control (MAC). The MAC address is the hardware address of a node in the network, such as a network adapter. By designating which MAC addresses have wireless access, unauthorized access is eliminated.

- Setting up the access point to stop broadcasting its Service Set Identifier (SSID). The SSID is part of the automated connection process that tells network adapters which 802.11b network it is joining. Only authorized users will know the SSID and security key, which are needed to establish a connection.

Internet communications that implement the secure socket layer (SSL) protocol will be encrypted, thus ensuring that the information is sent, unchanged, only to the intended server. Online shopping sites and banks use SSL technology to safeguard

sensitive information.

Table
Current Wi-Fi standards

Standard	Frequency	Theoretical transmission rate/typical rate (megabytes per second)	Range (meters/feet)
802.11b	2.4 GHz	11/4-6	30/1000
802.11a	5 GHz	54/20-25	25/75
802.11g (compatible with 802.11b)	2.4 GHz	54/6-24	30/1000

Related Resources

Wi-Fi Alliance: Wi-Fi Overview. Available at: http://www.weca.net/OpenSection/why_Wi-Fi.asp?TID=2. Accessed Nov. 18, 2003

If you have any questions about these products or comments about Psyber Psychiatry, click here to contact Dr. Luo or send an e-mail to Current.Psychiatry@dowdenhealth.com.

Disclosure

Dr. Luo reports no financial relationship with any company whose products are mentioned in this article. The opinions expressed by Dr. Luo in this column are his own and do not necessarily reflect those of CURRENT PSYCHIATRY.

REFERENCES (ALL URLS ACCESSED DEC. 2, 2003)

1. Wi-Fi FreeSpot Directory. http://www.wififreespot.com/
2. T-Mobile HotSpot. http://www.t-mobile.com/hotspot/default.asp?nav=hm
3. Boingo Wireless: 5,000 HotSpots. http://www.boingo.com
4. Warchalking http://www.warchalking.org
5. Borisov N, Goldberg I, Wagner D. Security of the WEP Algorithm. Available at: http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html
6. AirSnort. http://airsnort.shmoo.com/
7. Wireless networks. Does Wi-Fi Run Afoul of HIPAA? *Mobile Health Data* Sept. 7, 2003. Available at: http://www.mobilehealthdata.com/article.cfm?articleId=451
8. Nobel C. Wi-Fi to get big extensions. *eWeek* Dec. 1, 2003. Available at: http://www.eweek.com/article2/0,4149,1400188,00.asp