

December 12, 2002, Thursday

CIRCUITS

THE WI-FI BOOM; So Many Nodes, So Little Security

By GLENN FLEISHMAN (NYT) 742 words

WHILE driving along any Manhattan street, you would not expect strangers to fling their private correspondence and even their credit-card numbers at you as you passed by.

A recent survey of Wi-Fi networks, however, revealed not only the extent of Wi-Fi adoption -- covering more than 14,000 business and personal networks -- but also the apparent laxity of users about Wi-Fi's built-in security. Nearly 70 percent are using the networks in ways that, without other security measures, could expose every word and digit sent or received to potential interception and allow others to piggyback on their Internet service.

The survey's researcher, Marcos R. Lara, who has been active in establishing free Wi-Fi access in New York, drove along nearly every street in Manhattan over the summer using a combination of monitoring software that detected the presence of Wi-Fi networks and a Global Positioning System receiver to put virtual pins in a map.

Mr. Lara collected geographical snapshots of those networks, identifying available signals, network names, equipment manufacturers and security settings. Wi-Fi network equipment broadcasts many aspects of its identity even when configured to be invisible. Mr. Lara said he did not intercept data making its way through those networks nor try to connect to the access points his survey detected.

While e-commerce transactions are typically encrypted by the Web sites involved, other communications over unsecured Wi-Fi

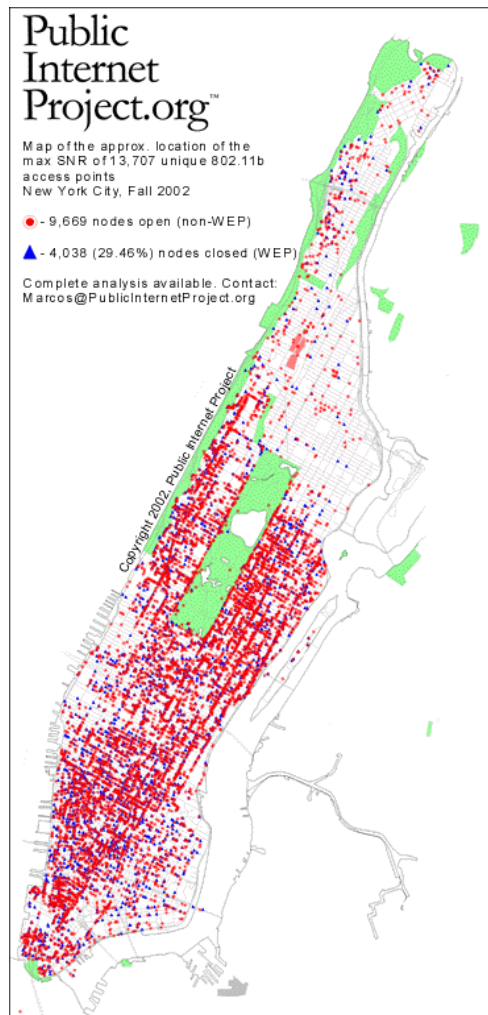


Photo: CONNECTED -- A survey found thousands of Wi-Fi networks in use in Manhattan, some of them public but many in homes and offices and most south of 96th Street. Thousands more access points are expected to be built in the borough in the next year. (Public Internet Project)

networks can easily be examined with freely available software, a Wi-Fi card and computers running the Macintosh, Windows or Linux operating system.

Only 30 percent of the networks discovered in Mr. Lara's survey had turned on the encryption system in their Wi-Fi programs, called WEP, to secure their data. And even that encryption is crackable with some effort. On unsecured networks, a passer-by or neighbor could record all traffic or gain uninvited access to local machines and an Internet connection. (Some of the private networks may use other security methods, like commercial firewall software or virtual private networks, that may protect data but leave the Internet connection open to freeloading.)

Why are so few of those using Wi-Fi at home bothering with its built-in security? Probably because in most systems, it is cumbersome. Many Wi-Fi programs require passwords up to 26 figures long, mixing numerals and letters. And it may take several typo-plagued attempts before the password is successfully entered.

Free and commercial public networks providing public Internet access in parks or coffeehouses are also typically unsecured, though users can employ security programs on their own computers.

But the number of purposely shared Wi-Fi networks is dwarfed by the number of private nodes. The survey revealed that 60 to 80 percent of the detected access points, or hot spots, used consumer-brand equipment, indicating that they were households or small businesses. NYC Wireless, a networking advocacy group, lists about three dozen free Manhattan locations, while T-Mobile has 100 fee-based hot spots. Several thousand commercial hot spots are expected to be built in Manhattan in the coming year.

Mr. Lara's survey, described at www.publicinternetproject.org, also found a stark dividing line between Manhattan's haves and have-nots: 92 percent of network nodes were below 96th Street.

Andy Carvin, an editor at the Benton Foundation's Digital Divide Network (www.digitaldividenetwork.org), noted that even technology advocates involved at the street level do not always know the exact picture of usage. "Activists in the digital-divide community realize the power of mapping because it helps us fill in the blanks of what's happening where," Mr. Carvin said.

"It's one thing for a local community activist to go to a member of Congress and say, 'We have a digital-divide issue in your district,'" and another to show them exactly what that looks like, he said. -NYT

By GLENN FLEISHMAN (NYT) 742 words