

---

# Law Practice TODAY

 [Print This Article](#)

## TECHNOLOGY

### Wireless Insecurity

by [Joe Kashi](#)

May 2004

Wireless networks are poised to take off in the business market because of recently lower costs and their apparent ease of installation, particularly where an older building makes the installation of hard-wired networking cable burdensome or expensive. However, they are very vulnerable to hacking and other security breaches. In this presentation, I'll discuss why I would not think of installing a wireless network in my own law office.

Among the purported benefits of wireless networks are increased flexibility, much lower installation costs, lower long-term maintenance burdens, and easy "hot desking" where users are highly mobile and need to physically share an office space or regularly rearrange the physical configuration of their office. Wireless networking is also particularly suited to conferencing where portable computers are used by most of the participants and to working arrangements where employees are frequently out of the office.

These advantages might seem to be compelling, but the threat of intrusion is a substantial deterrent, given current wireless standards as implemented by most manufacturers. Because of critical security vulnerabilities, wireless Ethernet networking (also called Wi-Fi) remains far more suited to a home-based family Internet sharing arrangement than to legal and medical office arrangements where confidentiality is not only ethically necessary, but legally mandated. The very ease of setting up Wi-Fi networks encourages their installation by casual users who don't have enough experience or technical savvy to recognize gaping security problems, let alone remedy them.

Wi-Fi technology is a broadcast radio technology that works on the same 2.4 gigahertz microwave radio band as modern cordless telephones and Bluetooth wireless devices built into many notebook computers. As a result, Wi-Fi has the same advantages and disadvantages as any radio technology.

On one hand, as with any radio signal, Wireless Ethernet technology is susceptible to interference from such simple obstructions as the foil backing of fiberglass wall insulation. It is also susceptible to innocent, but annoying, jamming and degradation from such mundane items as a bad florescent light ballast, lightning, a sparking electrical motor, or an older automobile with a bad ignition, all of which can cause "static" electrical noise which can degrade a Wi-Fi networking signal, or even render it unusable.

Conversely, Wi-Fi's networking transmissions are broadcast indiscriminately so that they may be directly accessible by an intruder or hacker whom you'll never notice in your parking lot, across the street, or in a different part of your building. Wireless hacking is so common that there are many Web sites and discussion groups devoted to the practice, from which the barely computer literate can

download enough freeware programs to overwhelm most small wireless networks.

Wireless technology is inherently much more susceptible to intrusion and hacking than an equivalent hard wired network where signals are not radiated indiscriminately to drive-by hackers and the network server and cabling are, or at least should be, physically protected from casual intruders. In contrast, a wireless network is potentially available anywhere within the range of its radio broadcast signals, which can range anywhere from 20 or 50 meters to as much as 500 meters when sensitive equipment is used on the other end. Even given a 50 meter signal radius, an intruder can be driving by or sitting in a car across the street intercepting your signals—and you'll likely be totally oblivious to such activity unless forewarned to implement sophisticated hacking detection technology.

Wi-Fi's security dilemma is fundamentally the same as radio signal intelligence and cryptography efforts by national security agencies. Human nature being what it is, even if you have some suspicions of intercepted communications, it's easy to disregard those concerns as vague. After all, even in the middle of all out war, the Japanese high command in World War II continued to believe in the invulnerability of their codes even after its catastrophic losses at the Battle of Midway Island and in the Solomon Islands strongly suggested that the U.S. was reading its mail. Because of their ability to convince themselves that their broadcast radio messages were safe from intrusion, Japanese radio codes did not materially change during World War II, to the enduring advantage of U.S. forces.

Unfortunately, hacking is in fact a very real and large problem. One need only run a basic firewall program and note the periodic intrusion attempts on any network that has an Internet connection to understand the even greater threat to a network where a user need only drive by your office to obtain a connection. Some analysts believe that as many as 30 percent of all Wi-Fi corporate networks have already suffered a hacking attempt. Wi-Fi networks are particularly vulnerable to drive-by hackers who will map Wi-Fi networks, a process called "war-driving." Of course, it's illegal to penetrate any computer system without authorization, but that stricture has not stopped decades of hacking into hard-wired systems where the chances of leaving traces and being caught are higher.

## **The Danger of Defaults**

Feel better because your Wireless access point box states that the product includes 128-bit WEP encryption? Even that's of potentially little use. A 2001 drive-by survey of 808 different London Wi-Fi networks using the current 802.11b Wi-Fi standard found that a staggering 67 percent of those networks did not use any encryption at all, probably because the network installer was either too lazy to work through the resulting configuration complications or because the wireless access point manufacturer simply did not turn on encryption as the default configuration. Most users accept the default configuration or a non-secure configuration in any event because that makes for faster, easier installation and that's how Wi-Fi networking has been promoted, as a faster, easier means of connecting computers.

Beyond the propensity of most users to stick with insecure setup defaults, there are other, less obvious, but still gaping security holes. Typically, in all but the larger cities, only one or two brands of wireless access points and routers will be readily available and the default password needed to access administrator privileges and complete control of these readily available wireless access points probably will not be changed. Hence, the potential hackers doesn't even need to ascertain your password to try hack into a wireless network using another computer—the hacker need only find a similar router and its instruction manual or download the instruction manual for that router from the manufacturer's Web site. The default administrator password, which I suspect 90 percent of all users will retain, will be very clearly set out. Similarly, the default SSID System access information is

typically not changed and is printed in the access point's instruction manual. Although newer Wi-Fi standards, such as 802.11g are now coming on the market, the need for backward compatibility with much more common 802.11b devices limits the implementation of more intrinsically secure standards.

## Hacker Freeware

There is a great deal of freeware software available for immediate download that provides even a novice with substantial tools to remotely intercept wireless network data transmission packets and after having collected enough of your "encrypted data packets," crack your encryption vector for 128 bit WEP. That allows a hacker to remotely read your files and transmissions as if they were directly connected to your network. One of the more sinister aspects of wireless hacking is that it doesn't necessarily leave footprints. To use such programs one need not be a deeply experienced computer engineer, but merely have some basic computing knowledge. Finding and downloading cookbook Wi-Fi hacking programs takes about ten seconds using any standard Internet search tool. Wi-Fi hacking software is available for Windows systems, Mac, Linux/Unix, and Pocket PC based systems.

Here is a small sampler of the more common freeware Wireless hacking software:

1. Airsnort, wireless network "tool" that passively monitors 802.11b networks, doesn't leave any obvious intrusion traces, gathers your Wi-Fi broadcast data packets and then analyzes them to decrypt the 128 bit WEP encryption key, assuming that you're even using that basic encryption. There are other similar war-driving "sniffer" programs such as Aerosol and Mognet, which includes the ability to directly view captured 802.11b packets.
2. Network Stumbler, a program that grabs broadcast W-Fi configuration information and audits a network and its attached computers and users. There's even a version for Pocket PCs called MiniStumbler.
3. pong.exe, which ascertains passwords, WEP encryption keys, and the actual MAC addresses of network adapters.
4. Ethereal, which allows a hacker to examine the live data stream from a Wi-Fi network or capture the data stream to a disk for later viewing.
5. WEPcrack, a decryption program that uses the latest discovered systemic weaknesses in the WEP encryption scheme.
6. Kismet, which can simultaneously identify multiple 802.11 networks.

These programs can be downloaded, for example, from <http://802.11-security.com/security/tools>. Readily available programs like these cut both ways. They're useful for illicit intrusion into your network but also as a means of independently checking your own Wi-Fi security. You might find it both enlightening and useful to download some of this readily available freeware yourself an attempt to hack into your own network to test its security. Similarly, if you have any indication that you might be vulnerable to hacking, then try some counter-hacking software such as Odessey or FakeAP, programs that hides your network's true access addresses by generating thousands of false and misleading access point addresses that confuse fifteen-year-old cookbook "script kiddies."

Often, the same Web sites that provide double-edged hacking/security audit tools also include links to commercial security products that ostensibly plug the same Wi-Fi security gaps that are exploited by programs posted. Be sure that any commercial vendor solutions you might consider has been rigorously audited by neutral parties.

Wi-Fi is not yet even a fully mature technology and yet even reasonably mature and proven technology like 30 year old UNIX or 10 year old 32 bit Windows typically has some security vulnerabilities, although these become increasingly more difficult for "script kiddies" as the obvious holes are plugged. One need only recall at the "extremely critical " security vulnerabilities still found in Internet Explorer 6 and in Microsoft Active Scripting as late as November 2003, or the SNMP holes found in Cisco's Wi-Fi software to develop a disconcerting sense of the potential vulnerabilities that remain in even thoroughly studied, mature software.

## **Other Fundamental WEP Security Flaws**

The 802.11b Wi-Fi encryption algorithm is now widely considered to be a systemically flawed implementation of the more general RC4 encryption algorithm. Once flaws are known in the algorithm, then specific decryption techniques can be devised to efficiently crack the encryption without the need for slow brute force cracking efforts. As a result, a longer encryption bit length does not necessarily provide additional protection. Unfortunately, because this is a systemic problem, it is not susceptible to easy solution. In other words, the principal Wi-Fi security protocol is fundamentally flawed. Commercial vendors essentially try to provide rather complicated patches to a flawed product.

Further, because devices on a basic Wi-Fi network use the same encryption key and SSID, then the compromise or physical loss of any connected device, particularly a laptop computer, compromises the entire networks and its encryption security. An alternative to basic hacking is to simply sniff the Media Access Address (MAC) that is a fundamental part of every Ethernet network card and then hack to that specific network device. To do this, you don't necessarily need to intercept radio packets. In fact, getting a notebook computers MAC address can be as simple as turning the notebook computer upside down and reading the Wireless MAC address sticker the that is often attached to the bottom.

Other wireless security attacks are simply variants of well-known cryptology techniques. For example, one can passively intercept and decrypt network traffic by using standard statistical analysis, an approach that has formed the basis for code cracking for a few hundred years and which is the basis of some freeware Wi-Fi hacking programs. One can actively attack the network by forwarding known plain text messages from an unauthorized mobile station and then cracking the WEP encryption key by comparing the known plain text with the WEP-encrypted broadcast version. One can trick an access points into accepting an unauthorized user and then granting administrative privileges, a form of attacking which is quite straightforward if a standard router's default administrator password is not changed. Or, one can use a little more finesse by employing standard Windows and UNIX hacking techniques such as buffer overflows.

After about a day's worth of traffic has been captured, a user with a sufficiently powerful notebook computer can analyze that traffic, build a dictionary deconstructing the encryption scheme, and then read network traffic on a the real time basis. As with the case of identity theft, old-fashioned methods, such as going through your trash or otherwise finding plain text documents, still work and may be sufficient to support a decryption attack on your network. The worst part is that with passive monitoring and remote capture of your Wi-Fi network's broadcast traffic, you'll never really know.

Another problem is that a single malicious user can readily saturate a Wireless Ethernet connection with a standard denial of service attack similar to those which have previously interrupted major Internet servers.

Let's not forget the possibility of internal breaches resulting from unauthorized Wireless points that are connected to a network by unsophisticated but well-meaning employees who may not understand

wireless network vulnerabilities. These access points may not have even rudimentary networking security enabled and can compromise your entire network. Similarly, it's well to recall that about 80% of the security breaches of hard-wired networks result from disgruntled and former employees, perhaps terminated from employment, who retain the information to get into your network without even coming on your premises. Unauthorized use by current and former employees is perhaps the biggest single threat to the security of any network, whether wireless or hard wired. It's simply easier for disgruntled former employees to get into a wireless network without leaving a trace.

These obvious and growing security problems threaten both our ethical obligations and also the basic commercial needs of confidentiality and assured data integrity. Even though any unauthorized intrusion into someone else's computer or network is clearly illegal and unethical, that's unlikely to stop someone otherwise inclined, particularly when remote Wi-Fi hacking greatly reduces the chance of detection.

One is led to the essentially inexorable conclusion that wireless networks cannot be trusted at this time as a means of connecting law office users with to each other and to the firm's data. Indeed, given that Wireless networks only use a standard CRC redundancy check for data integrity and given that the CRC check itself is susceptible to malicious attack, a wireless user cannot even be certain that data itself has not been damaged or altered, not to mention read. Under such circumstances, attorneys using Wi-Fi networks must be concerned about their potential liability under Graham-Leach-Bliley and sooner or later HIPPA in the instance of attorneys deal with confidential medical information and records.

### **Some Thoughts on Reducing Wi-Fi Vulnerability**

Change your system configuration defaults NOW to something that can't be ascertained in a readily downloadable manual. You might as well implement the WEP security if for no reason other than discouraging casual or unintentional interception and reading of the data that you're broadcasting to one and all within a 50 to 500 meter radius. Try a non-obvious encryption key and change it regularly.

Don't use a Wi-Fi network for any confidential information and isolate it from your confidential data using a tested and verified hardware firewall.

Download some of the cookbook Wi-Fi hacking programs and try to break into your own network. At a minimum, you'll have a better idea of your own vulnerabilities.

Physically protect all mobile and external devices that connect to your Wi-Fi network so that someone can't simply find the device's MAC Ethernet address as a means to hack into your system.

Run current and frequently updated anti-virus and personal firewall software on every wireless device. In fact, I won't be surprised to see wireless-specific viruses and worms specifically targeting Wi-Fi devices before the next ABA TECHSHOW. These would be particularly insidious because they would be broadcasting your data in such a way that a passively listening hacker couldn't be electronically ascertained.

Change your passwords and SSIDs regularly.

Some manufacturers, such as Cisco and Bluesocket, are beginning to address the inherent vulnerabilities of wireless networks, but the solutions are still not fully mature nor based upon generally accepted, interoperable IEEE standards. If you're interested in such devices, then check the

validity of the security audits performed upon them.

Even with these somewhat tedious protections, you can have no assurance whatsoever that anything sent across your wire across a wireless network is in being read by somebody sitting in a different building or vehicle a hundred yards away. You just don't know and is no ready way to ascertain that. For all practical purposes, Wi-Fi networking should be treated for the next year or two, at a minimum, as if it were a public conversation in a room crowded with strangers. Nothing confidential or potentially damaging should ever be mentioned.

[Top](#)

---

**Joe Kashi** is an attorney and litigator living in Soldotna, Alaska, who is active in the Law Practice Management Section and a technology editor for Law Practice Today. He has written regularly on legal technology for the Law Practice Management Section, Law Office Computing magazine and other publications since 1990. He received his B.S. and M.S. degrees from MIT in 1973 and his J.D. from Georgetown University in 1976, and is admitted to practice in Alaska, Pennsylvania, the Ninth Circuit, and the U.S. Supreme Court.

[Current Issue](#) | [About](#) | [Article Archives](#) | [Subscribe](#) | [Advertise](#) | [Contribute](#) | [RSS/XML](#) | [Contact](#)  
© 2003-2005 [American Bar Association](#) | [Privacy Statement](#)