



Locking Down Your Wireless Network

10100101011011010010101101010110110010101001
0100100110011001010100011100101010010
0100101110010010010101001001001
11101110010101001010101101010101
10100101011011010010101101010110110
01001001100110010101000111001010100100001010101

Locking Down Your Wireless Network

New York's Westchester County recently proposed a law requiring that businesses secure their wireless networks. The county mentioned that changing the default SSID and disabling SSID broadcasting require little effort. This is true, but by no means do those actions adequately secure your wireless network.

You can read and read about Wi-Fi security, but nothing will get the point across as efficiently as actually seeing what eavesdroppers can see on an unsecured wireless network. Understanding the importance of securing a wireless network requires you to be aware of the issues that can result from not securing your network:

Real-time Traffic is Compromised

- People can see what Web sites you're visiting.
- Login information to unsecured sites (non-SSL) is compromised, along with the content.
- Login information and content from services such as POP3 e-mail accounts and FTP connections is compromised.

Network is Open for Others to Connect

- Your Internet connection may be used for sending and/or receiving illegal information, such as spam, music files, or even pornography.
- Others can access any shared files on PCs or servers connected to the network.

A Wi-Fi Eavesdropper's Look

First, let's take a look at what a Wi-Fi eavesdropper can see when you send an e-mail over a wireless network without encryption. Here we have an e-mail (shown in Figure 1) from a computer on a wireless network with Microsoft Outlook using a POP3 account.

At the same time, we captured packets from the network on a laptop using a free tool called Ethereal. As shown in Figure 2, you're able to see exactly what was in the e-mail. Just imagine if this was an e-mail containing real sensitive information, and someone passing by in their car captured the wireless packets.

If that isn't bad enough, see what was captured in the packet trace shown in Figure 3 (next page) when we synchronized the e-mail. This sensitive information includes the login information for the POP3 account. It clearly shows the main server, user name, and password for the account.

To clarify, the administrator of this wireless network could have changed the default

Figure 1

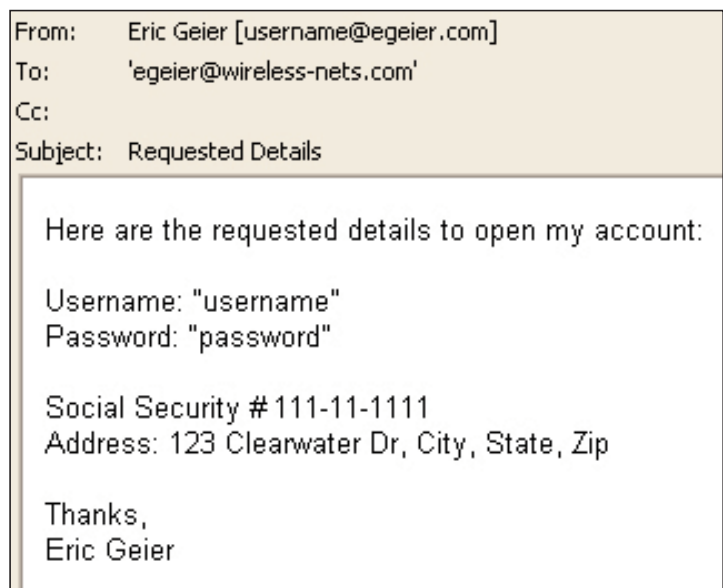


Figure 2

No.	Time	Source	Destination	Protocol	Inf
15	1.905373	192.168.:	64.40.144	SMTP	Co
16	1.958067	64.40.14:	192.168.1	SMTP	Re
17	1.985707	192.168.:	64.40.144	SMTP	Co
18	2.038330	64.40.14:	192.168.1	SMTP	Re
19	2.061594	192.168.:	64.40.144	SMTP	Co
20	2.113305	64.40.14:	192.168.1	SMTP	Re
21	2.139883	192.168.:	64.40.144	SMTP	Me
22	2.139934	192.168.:	64.40.144	SMTP	Me
23	2.139961	192.168.:	64.40.144	SMTP	...

Locking Down Your Wireless Network

SSID, disabled SSID broadcasting, enabled MAC address filtering, and many other things; however, we would still see the same information in Figures 2 and 3.

You should also note that we did capture these packets in Ethereal via an Ethernet connection to the test network. It is possible, though, to use Ethereal to capture packets using a wireless adapter. This brings up another issue: make sure the wired connections to your network are secure, because interlopers can capture any of the Ethernet traffic.

Figure 3

Source	Destination	Protocol	Info
192.168.1.1	192.168.1.1	NBNS	Registration NE
192.168.1.1	192.168.1.1	NBNS	Registration NE
192.168.1.1	Broadcast	ARP	who has 192.168.1.1
192.168.1.1	65.24.7.3	DNS	Standard query
65.24.7.3	192.168.1.1	DNS	Standard query
192.168.1.1	64.40.144	TCP	1968 > pop3 [SYN]
64.40.144	192.168.1.1	TCP	pop3 > 1968 [SYN]
192.168.1.1	64.40.144	TCP	1968 > pop3 [ACK]
192.168.1.1	192.168.1.1	NBNS	Registration NE
64.40.144	192.168.1.1	POP	Response: +OK <
192.168.1.1	64.40.144	POP	Request: USER U

Securing Your Private Wireless Network

Now that you understand the importance of Wi-Fi security, you should implement methods like those discussed below to ensure your sensitive information is secure.

To Secure Real-time Traffic

- Use WEP encryption at the minimum; ideally, go with WPA encryption.

To Prevent Others from Connecting

- Try to keep wireless coverage within a controlled area.
- Use MAC address filtering.
- Limit DHCP addresses, or assign static addresses.
- Disable SSID Broadcast.

Keep in mind that the use of encryption is the only method that adequately secures the real-time traffic, such as e-mails and Web browsing, on your wireless network. Most other security methods, such as MAC address filtering and disabling SSID broadcast, are intended to help prevent others from successfully connecting to the wireless network.

You can never be sure that your wireless network is completely secure. However, implementing multiple security methods means it will be much more difficult for Wi-Fi eavesdroppers to capture readable real-time data.

Protecting Yourself on Public Hotspots

When you're using an unsecured wireless network, such as a hotspot in a hotel, cafe, airport or any other public location, you should take steps to make sure your sensitive information isn't exposed:

Secure Your Real-time Traffic

- Use a VPN connection
- Make sure any services you use, such as POP3 and FTP, are secured if you are not using a VPN
- Don't visit any private or sensitive Web site unless it's secured (for example, implementing SSL) if you are not using a VPN

Prevent Others from Connecting to Your Laptop

- Disable any sharing of files, folders and services
- Use personal firewall software
- Make sure your operating system is kept up to date

A VPN connection encrypts any data sent from your wireless adapter all the way to the VPN server and vice versa, therefore providing end-to-end encryption. Along with providing a great way to secure the data, this also enables access to the remote network hosting via VPN server, which is often used in businesses. If your employer doesn't provide you with a VPN connection, you can either set up your own server, for example using Windows XP, or use a subscription-based, hosted service such as JiWire's SpotLock.

Securing Your Wireless Network

Wireless networking products are so ubiquitous and inexpensive that just about anyone can set up a WLAN in a matter of minutes with less than \$100 worth of equipment. This widespread use of wireless networks means that there may be dozens of potential network intruders lurking within range of your home or office WLAN.

Most WLAN hardware has gotten easy enough to set up that many users simply plug it in and start using the network without giving much thought to security. Nevertheless, taking a few extra minutes to configure the security features of your wireless router or access point is time well spent. Here are some basic things you can do to protect your wireless network:

1. Secure your wireless router or access point administration interface

Almost all routers and access points have an administrator password that's needed to log into the device and modify any configuration settings. Most devices use a weak default password like "password" or the manufacturer's name, and some don't have a default password at all. As soon as you set up a new WLAN router or access point, your first step should be to change the default password to something else. You may not use this password very often, so be sure to write it down in a safe place so you can refer to it if needed. Without it, the only way to access the router or access point may be to reset it to factory default settings, which will wipe away any configuration changes you've made.

2. Don't broadcast your SSID

Most WLAN access points and routers automatically (and continually) broadcast the network's name, or SSID (Service Set Identifier). This makes setting up wireless clients extremely convenient since you can locate a WLAN without having to know what it's called, but it will also make your WLAN visible to any wireless systems within range of it. As mentioned earlier, this disabling the broadcast of your SSID isn't difficult. Turning off SSID broadcast for your network makes it invisible to your neighbors and passers-by (though it will still be detectible by WLAN "sniffers").

3. Enable WPA encryption instead of WEP

802.11's WEP (Wired Equivalency Privacy) encryption has well-known weaknesses that make it relatively easy for a determined user with the right equipment to crack the encryption and access the wireless network. A better way to protect your WLAN is with WPA (Wi-Fi Protected Access). WPA provides much better protection and is also easier to use, since your password characters aren't limited to 0-9 and A-F as they are with WEP. WPA support is built into Windows XP (with the latest Service Pack) and virtually all modern wireless hardware and operating systems. A more recent version, WPA2, is found in newer hardware and provides even stronger encryption, but you'll probably need to download an XP patch in order to use it. We'll discuss WPA2 in more detail later.

4. Remember that WEP is better than nothing

If you find that some of your wireless devices only support WEP encryption (this is often the case with non-PC devices like media players, PDAs, and DVRs), avoid the temptation to skip encryption entirely because, in spite of its flaws, using WEP is still far superior to having no encryption at all. If you do use WEP, don't use an encryption key that's easy to guess like a string of the same or consecutive numbers. Also, although it can be a pain, WEP users should change encryption keys often -- preferably every week.

5. Use MAC filtering for access control

Unlike IP addresses, MAC addresses are unique to specific network adapters, so by turning on MAC filtering you can limit network access to only your systems (or those you know about). In order to use MAC filtering you need to

find (and enter into the router or AP) the 12-character MAC address of every system that will connect to the network, so it can be inconvenient to set up, especially if you have a lot of wireless clients or if your clients change a lot. MAC addresses can be "spoofed" (imitated) by a knowledgeable person, so while it's not a guarantee of security, it does add another hurdle for potential intruders to jump.

6. Reduce your WLAN transmitter power

You won't find this feature on all wireless routers and access points, but some allow users to lower the power of your WLAN transmitter and thus reduce the range of the signal. Although it's usually impossible to fine-tune a signal so precisely that it won't leak outside your home or business, with some trial-and-error you can often limit how far outside your premises the signal reaches, minimizing the opportunity for outsiders to access your WLAN.

7. Disable remote administration

Most WLAN routers have the ability to be remotely administered via the Internet. Ideally, you should use this feature only if it lets you define a specific IP address or limited range of addresses that will be able to access the router. Otherwise, almost anyone anywhere could potentially find and access your router. As a rule, unless you absolutely need this capability, it's best to keep remote administration turned off. (It's usually turned off by default, but it's always a good idea to check.)

The Lowdown on Wi-Fi Security

Wireless security protocols have improved considerably, despite the lackadaisical attitude of most users towards their computer security.

Road warriors must be especially careful. Public hotspots typically don't bother with WPA or WEP, or anything security-related at all. It is trivial to sniff an open wireless connection and perpetrate evil deeds like redirecting you to a fake WLAN login page, and then capture all of your secret stuff with ease.

Let's leap right into the definitions of the relevant standards:

```
802.1x-2004 Port Access Control for all LANs
802.11i-2004 Security enhancements for all wireless LANs
802.11a-1999 High-speed wireless 5 GHz
802.11g-2003 High-speed wireless 2.4 GHz
802.11b-1999 Wireless 2.4 GHz
```

802.11i is also known as WPA2, or Wi-Fi Protected Access. Both WPA and WPA2 use 128-bit encryption algorithms, and algorithm geeks engage in endless ferocious debates over their respective merits. WPA uses TKIP (Temporal Key Integrity Protocol), and WPA2 uses AES (Advanced Encryption Standard). WPA2 is a complete implementation of the IEEE's 802.1x standard for WLANs. WPA2 devices also support WPA; so if you're buying new gear, get WPA2. Don't worry about replacing WPA devices.

Wireless Device Support

Wireless access points and network interface cards must support WPA/WPA2. Many WEP devices can be upgraded with new firmware or drivers, and WPA devices should be upgradeable to WPA2. Some can't. The feeblest member of your WLAN limits you, so if you have any old non-WPA/WPA2 compliant devices still floating around, they need to be upgraded or jettisoned. Most 802.11g devices should be fine, it's the a and b devices that are the likeliest to need upgrading or replacing.

New wireless-G interfaces are inexpensive, but even so don't be in a hurry to chuck those old 802.11a/b NICs, because many of them are upgradeable if you are canny and can find the firmware and drivers. If your vendor does not provide upgrades, try the radio chip manufacturer, like Hermes, Proxim, and Agere. Just run `lspci` to get this information, and remember you can query Windows PCs the same way with a Knoppix CD.

The Wi-Fi Alliance requires that all devices that want to carry the "Wi-Fi CERTIFIED" mark must support WPA2, so they will be easy to find.

Operating System Support

Linux support comes via device drivers and user-space applications like wpa-suplicant. Mac OS X users merely need to have the latest AirPort or AirPort Extreme software. Windows users, as usual, have a more interesting time of it.

Windows XP users need Service Pack 2 and the "Wi-Fi Protected Access 2 (WPA2)/Wireless Provisioning Services Information Element (WPS IE) Update." Users of other Windows versions are on their own. There are third-party supplicants available, for a fee. Meetinghouse Data Communications' Aegis Client and Funk Software's Odyssey Client are the two that get a lot of mentions, and will cost \$40 to \$50 per user. Or, you may get lucky and your hardware vendor will include one with your wireless widgets.

What is this "supplicant" stuff? "Supplicant" is the official word in the standard, and all it means is WPA client software. It runs in the background and controls your wireless connections. Supplicant is an interesting word choice, with all of its overtones of humility and abasement.

Personal or Enterprise WPA

A nice feature of WPA allows you to choose from two levels of security, Personal and Enterprise. Personal is simple to implement, but it requires that all users be trustworthy. Everyone on the WLAN uses a shared key, which is the password, so they all share the same password. The key is entered into the router and all clients, and that's all it takes to set it up.

Enterprise mode requires a separate authentication server, like a RADIUS server. Enterprise mode is very flexible and should adapt to just about any existing authentication scheme.

WPA Gotchas

The WPA2 standard is a good thing, as it provides strong encrypted authentication, access controls, and encrypted data traffic. But it does not provide end-to-end encryption, it only encrypts the traffic between your wireless NIC and whatever wireless access point you are connecting to. WPA does not affect anything upstream. Once you log into your LAN, traffic is sent in the clear. When you leap out to the Internet, don't feel all comfy and secure, because that is sent in the clear as well. Except, of course, for the usual application-specific encryption, such as HTTPS, SSH, and TLS-SSL.

For ordinary Web-surfing and e-mail, this is probably not a big deal. But if you make a WAN connection to your remote company

Like all new technologies Wi-Fi has a good side and a bad side. In the case of London, Paris, and New York, the good side is a marked increase in the availability of hotspots. The bad side is many of these hotspots may be rouge-designed specifically to steal information.

And, if your mobile professional is tapping into, say, a client's internal Wi-Fi network, there's a 25% chance that network is not secured, according to research sponsored by RSA Security.

"It's definitely good news in the availability of wireless... but the flip side of that is you have make sure you are careful and protected," said Matt Buckley, communications manager for RSA. "Don't send e-mail, user names, passwords -- any sensitive personal data over an unencrypted link."

VPN and strong authentication are the best ways to do this, he said.

The largest year-on-year rise in Wi-Fi network usage was discovered in London, where there are 57% more wireless network access points than in 2005. The percentage increase in New York was an impressive 20%. In Paris, the increase from 2004 to 2006 was 119%.

And, in both London and New York, more businesses are securing their wireless networks by switching on the WEP encryption capability provided as standard.

In London, WEP usage rose from 65% in 2005 to 74% in 2006. For New York, WEP usage increased from 62% in 2005 to 75% in 2006. And Paris, which has the highest levels of encryption at 78%, posted an increase over 2004's figure of 69%.

This is an encouraging sign, said RSA, although in all cities, around a quarter of the wireless networks identified as belonging to and operated by corporate entities were found to have no security measures deployed.

London has the most to be ashamed of with 26% of business networks unsecured; New York is not far behind with 25% and the Parisians come in at 22%.

--Allen Bernard, CIO Update

network, it likely is a big deal. So you'll still need VPN tunnels or some sort of separate security for those situations.

Some devices that support both WPA and WPA2 do so only in Personal mode.

Configuring WPA for Linux

Let's look at how to configure WPA Personal on both Debian clients (and its many offshoots) and Red Hat (and its many spawn). Access points are diverse, so follow the vendor's manual for configuring them.

Setting Up WPA Personal

Setting up WPA-PSK (Pre-Shared Key) or WPA Personal is a nice solution for home and small business networks that don't want to hassle with an authentication server. Its main drawback is using a shared key, so if there are any generous blabbermouths on your WLAN who want to share your WLAN with their friends, you might want to restrict them to a wired host. The advantages are that it's easy to use, even across mixed environments, and it's secure, as long as you don't have blabbermouths.

On Linux you need `wpa_supplicant`. On Debian and its offspring it's `wpa_supplicant`. The configuration file is usually `/etc/wpa_supplicant.conf`.

The first step is to generate a strong passphrase. This is also your shared key. A WPA2 key can be up to 63 characters long. You might as well use all of them, because the encrypted key is going to sit inside `/etc/wpa_supplicant.conf`; you won't be typing it every time you want to login. Use the `wpa_passphrase` command. You need your WLAN's SSID and a bit of imagination:

```
$ wpa_passphrase myssid waylongkeythelongerthebetterbecausewecareaboutsecurityalot
network={
    ssid="myssid"
    #psk="waylongkeythelongerthebetterbecausewecareaboutsecurityalot"
    psk=ef82e334d941fd88ee8e6d6ef9d112eed40e93e2aa560fcaa326c29659ad375d
}
```

In reality that is not a good passphrase. It should not contain any dictionary words, and should be a combination of letters, numbers, and punctuation marks.

Copy your `wpa_passphrase` output into `/etc/wpa_supplicant.conf`. This exact same passphrase must also be on your access point and all other WLAN clients. Test your ability to connect, and once that's verified delete the line starting with `#psk=` because, obviously, storing your passphrase in cleartext is not a good security practice. Test it manually with these commands, using your own network interface name:

```
# iwconfig eth1 essid "myssid"
# ifup eth1
# wpa_supplicant -ieth1 -c/etc/wpa_supplicant.conf
```

There are no spaces between the option flags (`-i` and `-c`) and the options. Then verify that your interface picked up an IP and ESSID:

```
$ iwconfig eth1
```

Finally, ping a few sites to see if you have connectivity. And that's all there is to it.

Locking Down Your Wireless Network

Starting All This Stuff Automatically

Your users probably don't want to enter all these commands every time they want to connect to your network. So, if you're feeling benevolent, you can set everything up to start at boot. On Debian, Ubuntu, and the vast herds of other Debian-based distributions, edit `/etc/network/interfaces`:

```
auto eth1
iface eth1 inet dhcp
up wpa_supplicant -ieth1 -c/etc/wpa_supplicant.conf -Bw
down killall wpa_supplicant
```

-B forks the `wpa_supplicant` into the background, and **-w** tells it to do nothing unless the interface is up. On Fedora and Red Hat, et al., configure your wireless card in the usual manner in `/etc/sysconfig/network-scripts/ifcfg-eth1`, or whatever file belongs to the wireless interface, using the real interface name and MAC address:

```
DEVICE=eth1
BOOTPROTO=dhcp
HWADDR=11:22:33:44:55:66
ONBOOT=yes
TYPE=Ethernet
```

Then add these lines to the end of `/etc/sysconfig/network-scripts/ifup-wireless`, again using your own interface name:

```
wpa_supplicant -iath1 -c/etc/wpa_supplicant.conf -Bw
killall wpa_supplicant
```

These are simple setups that don't manage multiple locations or do any fancy hotplug management, but they work fine for single locations.

Security gurus suggest changing shared keys periodically. Doing it manually is less than fun. Using `cfengine` is one option, though that's a big hammer to use on a little nail. Your access point might have a utility to do this, so look there first.

Safeguard Your Laptop

Wireless networks and Internet cafes have made it more convenient than ever for the laptop-wielding road warrior to get online, but as the saying goes "nobody rides for free." You pay a price for this convenience and if you're not careful, it could be a high one.

Wireless hotspots are a hotbed for snooping and hacking. Malcontents clandestinely monitor wireless communications looking for any weakness in your security that would allow them to intercept whatever information you are broadcasting. In fact, without the proper protection, you could be broadcasting important business secrets and personal passwords to the guy sitting two tables over.

If you're accessing sensitive business files from a remote location, security is paramount. Without it, snoopers and hackers can follow you right into your network as easily as following a trail of breadcrumbs. Should that happen, you risk losing sensitive files or having your network brought down. Worse still, thieves could use the information to steal your identity.

Network security managers need to plan for, monitor, and recognize potential network breaches as well as react quickly when any breach occurs. To ensure effective, automated, wireless threat protection, companies and government organizations should implement a wireless intrusion detection and prevention (WIDP) solution that enables them to detect vulnerabilities, assess threats, prevent attacks, and ensure ongoing compliance - easily and cost effectively.

Hackers have developed a wide variety of tools to find and exploit WLAN vulnerabilities, including encryption and authentication cracking tools, war driving (using scanning and probing devices to search for unprotected WLANs), and long-range antennas to pick up 802.11 signals from a distance. New hacking freeware tools are introduced on an almost weekly basis. Hackers use these tools and others to launch a wide variety of assaults, including malicious association, identity theft, man-in-the-middle attacks, and denial of service attacks.

At a minimum, enterprises must encrypt and authenticate communications on the WLAN, but that is just step one. Even with a VPN in use, WLANs are vulnerable to many advanced attacks that prey on the inherent loopholes in these security implementations. At first blush, traditional approaches for detecting network vulnerabilities and attacks seem viable for the WLAN domain. But with further examination, it becomes clear each has severe flaws that make it unsuitable for protecting the WLAN from intrusions.

By deploying a dedicated wireless security system that monitors the wireless communication channels, an enterprise can more effectively respond to WLAN security issues. While off-the-shelf AP hardware is limited to scanning one region at a time, it is critical to scan the more than 220 802.11a/b/g channels in the regulatory domains of the U.S., Europe, and Asia, plus the "gray" channels defined in this spectrum. Gray channels, which rogue devices trying to evade detection can use, are increasingly configurable with off-the-shelf wireless equipment.

The ability to scan gray channels is particularly important to global organizations, where employees are more likely to introduce "off-region" rogues. If an enterprise is not currently using a dedicated wireless security solution, it will not know how effective its security architecture is until it is too late. Even organizations with "no wireless" policies still need to monitor their airwaves if they want to enforce such policies.

While detection is the first step, it is also where the first generation of solutions, including the part-time security capabilities built into traditional APs, stop. Organizations need a dedicated system to actively prevent attacks. A purpose-built WIDP system provides the critical next step needed to automate threat protection. Such systems automatically respond to wireless threats based on how policies have been set to best meet enterprise business objectives.

-- Brian de Haaff, Wi-FiPlanet

While security is a problem for everyone, you're at even more of a risk if you work out of remote locations like hotels and cafes. Not only do you risk losing data through wireless communications, but a Safeware Insurance survey found that more than 600,000 laptops were stolen in 2004 alone.

This leads to the obvious question: How do you prevent your information from falling into unauthorized hands? You could stay off of the Internet entirely, but in most cases that's just not practical. And let's face it, no matter how careful you are, whenever you travel with a laptop there is always a chance that it could be lost or stolen. Thankfully, though, there are many companies out there that offer data encryption tools that should help minimize the risk to mobile warriors. Let's take a look at some of the options available to you for protecting your precious data.

Protecting the Files on Your Notebook

Let's start with the physical side of things. For starters, one of the simplest and easiest precautions to take is to set up a BIOS-based password on your system. This password needs to be entered as soon as the PC is booted. Another simple option is to set up a Windows user password. This would prevent an unauthorized person from gaining access to your personal data. Neither of these methods is foolproof, but they are already on your system and easy to implement.

Encrypting the data on your hard drive is a stronger solution. Fortunately, there are a number of software-based solutions on the market that will encrypt files on your notebook's hard drive so that prying eyes can't see them. These range from symmetrical key-based solutions to encrypted zip storage solutions. A symmetrical key solution is one that uses the same encryption "key" to encode and decode files on your hard drive. The key itself is password-protected, which prevents anyone without the password from viewing these files.

PGP Corp. offers both a home and a professional desktop package that provides encryption for your entire system. Its Virtual disk feature secures files, folders, USB drives, and CDs. It automatically encrypts mail and digitally signs your e-mail and attachments. It will even secure your AOL IM sessions. The only downside to this system is that it can be a bit expensive (\$99 for the home version and roughly \$200 to \$250 for the professional version), but if you're looking for security, this is one of the best ways to go.

Locking Down Your Wireless Network

A less-expensive solution is to compress confidential files on your hard drive and encrypt them during the compression process. Many of today's compression utilities (e.g., WinZip, BitZipper) feature advanced encryption capabilities that prevent compressed files from being viewed without the encryption key. This isn't an ideal solution if you're frequently accessing these files on your hard drive, since you don't want to compress and uncompress them every time you work on them, but it's a great solution for archived files and large files that you want to send over the Net. When sending compressed, encrypted files as an e-mail attachment, the recipient doesn't necessarily need the original compression application to open the file, as many of the latest compression utilities are compatible.

The Wireless Guardian

Although there are tools that can alert you when someone is trying to peek at your files and e-mails, the best defense is seamless data encryption. Some e-mail applications feature built-in data encryption, others don't, so check with your e-mail application vendor before deciding what gaps you need to fill.

For the best protection, 128-bit or higher AES protection is virtually impossible to crack. It places an impenetrable wall of encryption around the data you send and receive online, from e-mails to passwords.

Using instant messaging in a public Wi-Fi area is a more risky proposition, though presumably you're not using IM to communicate business secrets. Software tools can provide some level of security during public IM sessions, but only if the person on the other end is using IM protection, too.

In addition to AES, one of the most powerful tools available to the mobile warrior is a VPN. A VPN acts like a private tunnel connecting two or more points across the Internet. All data sent back and forth over the VPN is encrypted, including the destination and sender information, making it nearly impossible (or at least extremely unlikely) that any unauthorized person would be able to intercept them.

In order to provide privacy on the Internet, VPNs address security at three different places: on the client side (i.e., the remote user), during the actual transmission of data over the Internet, and at the gateway of the network itself. Using a VPN, employees can log onto a LAN from anywhere in the world, safely and securely with the same speed and convenience as if they were actually sitting there in the office. In this way, mobility doesn't cost you productivity.

The Internet is the world's largest network, but it's also the world's least private network. By combining various security measures with a bit of common sense, you could be ensured that your data will be safe and secure regardless of whether you're sitting at your desk or if you're relaxing at your favorite coffee shop.

This content was adapted from internet.com's Wi-Fi Planet Web site and EarthWeb's Practically Network Web site. Contributors: Ronald Pacchiano, Eric Geier, and Carla Schroder. Copyright 2006, Jupitermedia Corp.

JupiterWeb eBooks bring together the best in technical information, ideas and coverage of important IT trends that help technology professionals build their knowledge and shape the future of their IT organizations. For more information and resources on IT security, visit any of our category-leading sites:

www.esecurityplanet.com
www.antonline.com
www.internetnews.com/security
www.earthwebnews.com/security
www.enterpriseitplanet.com/security
www.insideid.com
www.smallbusinesscomputing.com
www.linuxtoday.com/security/

For the latest live and on-demand Webcasts on IT security, visit: www.jupiterwebcasts.com/security