



## Wi-Finally: wireless security that actually works

By Brian Livingston

**The security of Wi-Fi has largely been a joke. Wireless vendors have routinely shipped their products with all of their security features turned off, rather than take support calls from end users when things didn't work. Fortunately, the pieces are now in place for you to have safe and secure Wi-Fi networking, wherever you may roam.**

The latest piece to arrive is Microsoft support for WPA2 — Wi-Fi Protected Access 2. With the release of WPA2 client software for Windows XP earlier this month, you can now use the strongest form of Wi-Fi protection available without downloading third-party software. (Inexplicably, Microsoft's client doesn't support Windows 2000 or any other version of Windows. I'll explain below how to achieve protection on non-XP systems.)

When Wi-Fi routers, access points, and adapters first became available in "b" versions (technically known as IEEE 802.11b), the only form of built-in security available was WEP — Wired Equivalent Privacy. This algorithm, however, was quickly cracked by hackers. WEP today is useless, since common hacker tools can discover its security key within minutes, if not seconds. This is now also true for so-called dynamic WEP (also called WEP with IEEE 802.1X), in which the key changes every few minutes. Neither WEP nor dynamic WEP can be relied upon.

With the widespread availability of WPA2, however, I can now whole-heartedly endorse the use of today's fast "g" Wi-Fi (802.11g). Of course, that's only if you enable its Wi-Fi Protected Access features.

The good news is that Wi-Fi manufacturers have built secure capabilities into almost all modern equipment. "There's nothing that's been sold from early 2003 on that cannot be upgraded to WPA," says Glenn Fleishman, editor of [Wi-Fi Networking News](#), "as long as they're from the major manufacturers: Linksys, Belkin, Apple, etc."

The bad news is that you'll almost certainly have to turn these features on for yourself. Let's walk through exactly how that's done, shall we?

### What's wrong with unprotected Wi-Fi?

Many people wrongly assume, "I'm not doing anything important enough for hackers to care about." In reality, you have a lot to be concerned about if you use Wi-Fi without security turned on:

- **Unauthorized access.** Three hackers were sentenced to up to [12 years in prison](#) last year for using Wi-Fi to access credit-card data in a Lowe's hardware store in Detroit, Michigan. You may think you don't store credit card information on your laptop. But how much do you want to bet that a credit card number, Social Security number, password, or other personal data isn't located someplace on your hard disk?
- **Zombie networking.** Anyone near you can use your Internet connection in any way they wish if you're unprotected. This includes mass distribution of spam, kiddie porn, or denial-of-service attacks. All of these things would appear to have come from your computer — because they did. Hackers with powerful antennas can use your signal from [miles away](#).

• **Legal liability.** If an unsecured Wi-Fi connection is used for nefarious purposes, the issue of who's legally responsible is still being worked out by courts around the world. But attorney Robert V. Hale II published a [paper](#) last month indicating you might be held liable in such a case. In the article, published by the Santa Clara Computer and High Technology Law Journal, he argued that people who allow unprotected Wi-Fi might be found to have given "apparent consent" to anything that's done with the signal. Whether such a ruling would actually occur is anyone's guess — but do you want to be the test case?

## Throw out all your old Wi-Fi junk

For all of the above reasons, I've been leery of older, nonsecure Wi-Fi technology. To limit my exposure, I've emphasized wired Ethernet access in my office and configured a secure, virtual private network (VPN) for use in hotel rooms while traveling. (More on VPNs below.)

Now that WPA2 is widely supported, I've banned from my office all obsolete "b" equipment that can't use WPA. (That goes for incompatible 802.11a equipment, too.) Wi-Fi "g" equipment is now a commodity that's priced low enough to justify upgrading. For example, a 2-year-old Sony Vaio laptop I own had only "b" capability built in. I found a mini-PCI replacement card — an Intel PRO/Wireless 2200 BG, fully certified for WPA — for [less than \\$29](#).

If you have old "b" equipment that can't be upgraded to support WPA, it's garbage. Throw it out and replace it. The cost is justified. The risk of using nonsecured Wi-Fi is not.

## Security comes in two flavors: WPA and WPA2

Because the uselessness of the original WEP scheme quickly became obvious, the Wi-Fi Alliance trade group approved an early version of Wi-Fi Protected Access (WPA) in October 2003. An expanded standard, known as WPA2, was given formal approval in September 2004. Here's the difference:

• **WPA** uses 128-bit encryption called TKIP (Temporal Key Integrity Protocol). WPA is a subset of the official IEEE 802.11i standard.

• **WPA2** uses 128-bit encryption called AES (Advanced Encryption Standard), also known as CCMP (Counter-Model/CBC-MAC Protocol). WPA2 is a full implementation of IEEE 802.11i.

Whew. These people sure love their acronyms.

I consider both WPA and WPA2 to be secure methods of communicating using Wi-Fi. If you have equipment that supports only WPA, not WPA2, it's safe to continue using WPA. If you're buying new equipment, however, you should buy products that support WPA2. (Such products also support WPA.)

AES was selected by the U.S. National Institute of Standards and Technology (NIST) in 2000 as the winner of a competition to find the most secure encryption algorithm. Fifteen semifinalists from 12 countries were considered. AES encryption is required by U.S. governmental agencies and is considered secure enough that it's used in military applications.

TKIP is perfectly adequate to protect ordinary Wi-Fi transmissions, however. AES was added to WPA to meet the needs of customers who communicate with the U.S. government and others who require this specific algorithm.

Note: University of Illinois associate professor Daniel J. Bernstein published a cautionary paper on AES earlier this month. He demonstrates that many implementations are vulnerable to an insider on a network. By sending millions of data packets, the insider can narrow down and

ultimately guess the encryption key being used on a general-purpose CPU via a *cache timing attack*. In the paper, Bernstein promotes his own Salsa20 cryptographic function, which he says is easier to implement than AES.

"Pretty much any encryption algorithm is susceptible to timing attacks, so choosing on that regard doesn't make that much sense," said cryptographer Bruce Schneier in an e-mail interview.

"Resistance will depend in the physical implementation of the encryption algorithm, and not on the protocol choice." The threat doesn't seem to be imminent, but it bears watching. For more information and a link to the paper, see [Schneier's blog](#).

## Authentication is either Personal or Enterprise

Both WPA and WPA2 support two vastly different ways for users to identify themselves to wi-Fi routers and access points as authorized: Personal and Enterprise.

- **Personal Mode** requires a pre-shared key (PSK). This key is, ideally, a long, complex password that's entered into both a Wi-Fi router and any clients that are expected to connect to it. Generally, the same password must be used in the router and in all the clients that the router will talk to. This makes the PSK approach useful only for home users or small businesses, hence the name Personal.

- **Enterprise Mode** requires some form of logon to an authentication server. This could be a username/password combination, a secure token, or other logon methods. Enterprise Mode uses IEEE 802.1X authentication in a secure manner to verify the client to the router and the router to the client.

Some Wi-Fi products support both WPA and WPA2, but only in Personal Mode, not Enterprise Mode. If you're buying new equipment, I recommend that you invest in products that support Enterprise Mode. (Such products also support Personal Mode.)

Setting up an authentication server to work with WPA or WPA2 is beyond the scope of this article. The details are described in a 23-page PDF report from the Wi-Fi Alliance entitled [Deploying WPA and WPA2 in the Enterprise](#).

To help you find products that are certified to work with WPA and WPA2 in Personal and Enterprise Mode, the Wi-Fi Alliance has set up a useful database. The association tests each product to ensure that it interoperates with others that support the same level of compliance. You can then indicate the standards you want, and the site displays a list of all products that have been certified to comply.

For example, to look for Wi-Fi access points that support WPA2 and Enterprise Mode, simply select **Filter Products By Access Point**, check the box for WPA2-Enterprise, and click Submit. All matching products are then listed. Vendors have strong incentives to get certification (they can then display certified logos on their packaging, for instance), so the database is a fairly good representation of compliant products. To use the database, visit the Wi-Fi Alliance's [Certified Product Listing page](#).

For even better certification of Wi-Fi products, an intensive testing program has been announced by ICSA Labs, a respected independent research firm. ICSA requires products claiming WPA2-Enterprise compliance to meet a series of tests that are more demanding than those of the Wi-Fi Alliance.

ICSA launched its program as recently as May 5, though, so only one product has been certified to date (the Aruba 2400 Mobility Controller, in case you're interested). But the effort bears watching for those who want only the utmost in security. See ICSA's [Certified Wireless Products Listing page](#).

## Use a long key, such as 32 characters

If your Wi-Fi usage will be in a home or small business, and you can trust each Wi-Fi user not to give out your pre-shared key, the PSK method of authentication may be adequate for your needs. Be aware that anyone who knows the PSK can (with hacker software) decrypt and read other users' traffic, so this isn't a safe method for security-conscious businesses. It should be fine to use a PSK to support a few home or small-business users, though.

If you decide to rely on a pre-shared key and not set up an authentication server, however, you need to follow an important rule:

- **Make up a key that's (A) substantially more than 20 characters long and (B) doesn't contain any names or dictionary words.**

Robert Moskowitz, senior technical director of ICSA Labs, has written an [article](#) explaining that PSK is "almost as bad as WEP" unless "only truly random keys are used." A dictionary attack against a key that's merely a word or phrase "should be easier to execute than the WEP attacks," he says.

Since you rarely need to type the pre-shared key after it's been entered into a Wi-Fi router and its clients, you can make the key both long and strong. That means using lots of numerals and punctuation marks, and both upper- and lowercase letters. Don't even try to remember it by heart. (You should write down or print a copy of the key and store it in a safe place, obviously.)

One way to make up a strong key is to open a book and select a paragraph at random. Then write down the first letter of each word while randomly changing some of the letters to numerals, punctuation marks, and uppercase.

Or you can use a free online service, such as the WinGuides Password Generator. You specify the length you desire for your new key, such as 32 characters. You then turn on all of the service's check boxes, such as **Include Punctuation**. When you click **Generate Password**, the service creates a strong key, complete with a nonsense sentence to help you definitively identify each character. For details, see [WinGuides](#).

As the ideal solution, companies such as Atheros, Broadcom, and Buffalo have proposed and are implementing simple ways to generate strong keys. This includes push-button devices that do the work for you automatically. Unfortunately, these aren't yet universal. For more information, see Fleishman's [discussion](#) of these methods.

## Three essentials: client, adapter, and router

Now we get to the heart of the matter: upgrading your Wi-Fi components to support WPA or WPA2.

To successfully establish a WPA or WPA2 session, three of your components need to support the standard:

- **Client software.**
- **Wi-Fi adapter.**
- **Wi-Fi router (or access point plugged into a router).**

I'll briefly touch on the process of installing or upgrading these components, below.

## Use Microsoft's or a third party's WPA2 client

Just to lay one more dose of jargon on you, the Wi-Fi Alliance refers to client software that supports WPA/WPA2 as a "supplicant." This word ordinarily means "someone who prays for favors." You may well feel like doing this if your Wi-Fi system doesn't immediately work as expected.

Anyway, Microsoft's new WPA2 client software should work with most or all WPA and WPA2 equipment, since Wi-Fi Alliance certification supposedly tests for interoperability. If you use Windows XP, it can't hurt to download and install Microsoft's WPA2 client. It integrates seamlessly into XP's existing **View Available Wireless Networks** window. If you've succeeded in connecting wirelessly via WPA or WPA2, then "WPA" shows up in the description of the Wi-Fi network.

Microsoft's WPA2 client is available through Knowledge Base article [893357](#). Don't confuse this with an older WPA-only client, which is described in KB [815485](#).

If you use a version of Windows other than XP, you'll have to download a WPA2 client from a third party. Two such clients that are highly regarded are:

- [Funk Software's Odyssey Client](#) (free 30-day trial, \$50 single-user license).
- [Meetinghouse's AEGIS Client](#) (free 30-day trial, \$40 single-user license).

## Upgrading your Wi-Fi adapters and routers

There are so many different brands of Wi-Fi adapters, routers, and access points — each with its own upgrade procedures — that it's impossible for me to describe them all in a meaningful way here. Instead, if you need help with this process, I recommend you read an old article on upgrading Linksys equipment to WPA that was published in the Oct. 14, 2003, issue of [PC Magazine](#). (Caution: That article links to the older, WPA-only version of Microsoft's client software.)

In general, the best place to look for details on how to upgrade a specific brand of hardware will be at that company's Web site. That's easier said than done, I realize. At the Linksys site, for example, there's nothing about WPA or WPA2 on the company's home page. Entering **WPA2** in the home page's search box returns no results. The trick is to click the Support tab, then the Knowledge Base link, then enter **WPA** into *that* search box. Sheesh.

Some older Wi-Fi equipment lacks support due to the fact that the brand on the box has gone out of business. That's a shame, since some "b" cards that were sold as early as 1999 can actually be upgraded to support WPA (but not WPA2). If you're in this situation, see Fleishman's page on [older 802.11b cards](#).

## Internet cafés: open-air identity theft

The above steps will protect you when you're using Wi-Fi in your own home or office. But what about when you need to use a laptop wirelessly in a hotel or an Internet café?

Unfortunately, most public hotspots have never turned on any security features and probably won't for some time. One major exception is T-Mobile, which manages hotspots at more than 15,000 locations in 19 countries, including Starbucks, Borders Books, FedEx/Kinko's, and Hyatt Hotels. T-Mobile now supports WPA in all of its sites and no longer supports WEP, according to the company's [security statement](#).

On the down side, T-Mobile charges \$39.95 per month to use Wi-Fi at its locations. That's fine if your company is paying. If it's not, and you rely on free Wi-Fi access, you can protect yourself

(even on unsecured wireless) by setting up a private virtual network (VPN).

If you work for a corporation that's already set up a VPN, this step may have already been taken care of for you. If you're planning to set up a VPN for the first time, a good introduction to two popular flavors — IPsec VPNs and SSL VPNs — is provided in a recent [TechTarget article](#).

For home users and small businesses, creating a VPN from scratch is a daunting task. Fortunately, there are now low-cost services that will create and maintain a VPN for you, eliminating the technical work. Four of the players are:

- [HotSpotVPN](#) (\$8.88/month)
- [JiWire SpotLock](#) (\$4.95/month)
- [PublicVPN](#) (\$5.95/month)
- [WiTopia PersonalVPN](#) (\$79/year)

Of these four, HotSpotVPN has been in business the longest (three years) and supports the largest number of platforms (including Pocket PCs, Palms, Treos, and others). When comprehensive tests are conducted on these services by trusted reviewers, I'll publish the results in future newsletters.

Lest you think you're "just" surfing the Web or "just" checking your e-mail at a hotspot — and therefore don't need any security — you should know about the latest threats. These include "evil twins" — hacker Wi-Fi servers that display logon pages that look exactly like the ones your local hotspot displays. You log in, just like you always do, and then surf the Web. You're handing over your hotspot password and any number of other valuable passwords to the perpetrators. WPA and WPA2 prevent this kind of identity theft.

Whenever you use a public hotspot, you should always ask, "When will you support WPA2?" The counter clerk may not know what you're talking about, but you can request that your question be sent upstairs to management. For more information, the Wi-Fi Alliance explains how public hotspots can implement WPA2 and still support nonsecured users in a [PDF white paper](#).

## Should you buy G, Super-G, or MIMO?

If you're considering buying all-new Wi-Fi equipment, you'll find a confused market, with three conflicting alternatives. We might call these Standard G (fast), Super-G (somewhat faster), and MIMO (somewhat faster with better range).

Evaluating all these competing products isn't the purpose of this article, but you can examine the extensive tests of major Wi-Fi products published in the June 7, 2005, PC Magazine (which isn't yet posted on the Web at this writing). The reviewers awarded the magazine's Editors' Choice to three Linksys models, one in each speed category. (For more information on these Wi-Fi router reviews, see this issue's [Index of Reviews](#) and [Security Baseline](#) columns.)

The routers that claim the fastest throughput, called MIMO routers, cost several times the price of Standard G routers. I believe Standard G equipment pencils out as the most cost-effective upgrade for home users and small businesses at this time. Such routers should give you adequate throughput and range if your Wi-Fi usage occurs mainly in one or two rooms of your home or office.

If you need greater range than that, consider buying a MIMO router but not purchasing special, high-priced MIMO adapters. Fleishman, who's tested numerous setups, finds that ordinary, low-cost "g" adapters do gain a benefit from the extra range that the expensive MIMO routers provide. There's no boost in throughput when using the simpler adapters, but if you're primarily using Wi-Fi just to access the Web, your broadband connection (typically 2 or 3 Mbps) will never get close to saturating a Wi-Fi router (about 20 Mbps, real world).

If ordinary "g" equipment satisfies your needs for now, super-fast 802.11n equipment will be a better future upgrade path than MIMO. High-speed 802.11n devices are expected to ship in early 2007. Today's MIMO products, despite their "pre-N" advertising pitches, won't be upgradable to 802.11n and won't be compatible.

### **The top six steps you shouldn't bother with**

With all the details given above, using Wi-Fi securely may seem to you like an enormous undertaking. If so, take a deep breath and plunge ahead. I can at least save you from *some* grief by listing a few things that *won't* help your security. They'll just waste your time.

George Ou, a columnist for ZDnet, has provided us with a fascinating rant against "The Six Dumbest Ways to Secure a Wireless LAN":

- **MAC filtering.**
- **SSID hiding.**
- **LEAP authentication.**
- **Disabling DHCP.**
- **Interior antenna placement and low power.**
- **Limiting your use to 802.11a or Bluetooth.**

He argues persuasively that all of the above techniques are useless in securing your Wi-Fi system. He barely mentions WEP, reiterating that it can be cracked in [minutes](#). For more details, see Ou's [list of the dumbest ways](#).

There's much more, but I'll stop here for now. To send us more information about WPA or WPA2, or to send us a tip on any other subject, visit [WindowsSecrets.com/contact](http://WindowsSecrets.com/contact). You'll receive a gift certificate for a book, CD, or DVD of your choice if you send us a comment that we print.

Brian Livingston is editor of the Windows Secrets Newsletter and the coauthor of [Windows 2000 Secrets](#), [Windows Me Secrets](#), and eight other books.