

Step-by-Step Guide: Locking down laptops that connect to hotspots

By Kevin Beaver, author "Hacking Wireless Networks for Dummies"

Connecting to the Internet at a wireless hotspot can be hazardous to your computer's health. Even worse, your (and your organization's) sensitive information can be put at serious risk if your computer and communications channel are not locked down and protected against the elements whenever you log on at your favorite local hotspot.

A controlled network environment is bad enough, but when you're connected to the Internet wirelessly among a bunch of strangers, it's like swimming among sharks -- you never know when someone is going to attack. This is true in "open access" hotspots (which I'm seeing more and more of) and even at "trusted access" hotspots that require you to subscribe and authenticate before obtaining access.

All it takes is someone with a wireless network analyzer to see what's going on. Add to that a few basic hacking tools and your computer can be "owned" by someone else in a matter of minutes. Take the following steps to ensure that your wireless laptop is locked down. That way you can keep the good stuff in and the bad guys out the next time you connect wirelessly in a public place.

Step 1. Understand what there is to lose and who's stealing the loot

When we're inside a coffee shop or any other public hotspot including airports and hotels, there's a lot of "juicy" wireless communication going on -- most of which is very easily intercepted. There's so much for us to lose and for the bad guys to gain in the form of e-mail, instant messages, files stored on laptop drives and more. The possibilities are endless. They include identity theft, loss of sensitive corporate information and the installation of malicious software that tracks our every action on the computer. What about that person who blackmails you when he finds some dirt on you? Something like that can be a real life-changing event!

When it comes to the people who are actually doing the bad stuff, you may be surprised. A hacker, we tend to think, is the stereotypical pimple-faced teenager pecking away on a keyboard in a school lab instead of that nicely dressed young man sipping a latte at the table next to us in the local coffee shop. The truth is that we don't really know who is out there poking and prodding our computers maliciously. However, based on people I've seen and heard -- even from self-proclaimed security professionals -- a lot of people are doing bad things to other people's unsecured data in hotspot settings.

Malicious intruders who have nothing better to do can easily listen in on instant messaging (IM) conversations. They can watch Web browsing in real time, and they can even poke around on unsuspecting users' computers. Given how simple these attacks are to carry out, it's amazing that most people are not doing anything about it.

Step 2. Secure your computer to prevent attacks in the first place

Install the basics: There are several things you can do to ensure you keep the bad guys and their malicious software out of your system. For starters, keep up with patches -- either manually or via Automatic Updates or other automated patch management system. Also, have antivirus and antispymware software installed. Most people have the former type of protection but (still!) very few have the latter. If you're on a budget, at least check out Microsoft's AntiSpyware solution -- it's had good reviews, seems to do its job and it's free.

Protect the operating system: It's one thing to protect a communications link, but it's entirely another thing to protect your actual computer. Why? Well, that's where the "money" is -- files, password hashes and other stuff that tends to pique the interest of the bad guys.

Perhaps the most important piece of software to help protect your computer is a personal firewall. It is, hands down, the best way to protect your systems from remote access. Try Windows Firewall built into XP SP2 and later, or check out one of the freeware or commercial products like ZoneAlarm, from Zone Labs LLC or, my favorite, BlackICE from Internet Security Systems Inc. Once you install a personal firewall, just be careful about the rules you set up, as it's easy to tweak your system to inadvertently allow external Windows access.

Don't forget about ad-hoc clients: Many laptops with wireless cards are vulnerable even if they're not connected to a hotspot. These systems have their wireless network card running in what's called ad-hoc mode. Ad hoc, sometimes called peer-to-peer mode, enables wireless clients to communicate with each other without a wireless access point (AP) to facilitate everything. Check your wireless settings and ensure ad hoc is not enabled if you don't need it. Otherwise, it may be possible for an attacker to join your ad-hoc network and muck around on your system.

Step 3. Secure your communications link

Wired Equivalent Privacy (WEP) and WiFi Protected Access (WPA) are nice but, unfortunately, most hotspots don't support these security protocols. They're just too difficult to manage in a public environment. If you're connecting into your home or corporate computer from a hotspot, make sure you connect via a secure VPN -- not just Windows Terminal Services, remote desktop or some half-baked remote connection. A great VPN solution that's free and easy to set up in Windows environments is point-to-point tunneling protocol (PPTP). It's built into Windows server-based systems and you may even be able to get it to work in Windows 2000 and XP Professional as well.

To protect your e-mail communications, enable S/MIME or PGP within your e-mail client. You can also use secure POP (via TCP port 995 instead of port 110) for e-mail downloads and secure SMTP (via TCP port 465 instead of port 25) for sending e-mail. Many current e-mail clients support these two types of secure e-mail links with the caveat being that the server on the other end has to support them as well. If instant messaging is your way of communicating, many IM clients allow for secure communications using digital certificates and Secure Sockets Layer/Transport Layer Security (SSL/TLS).

When it comes to Web browsing, a snooper can track most sites, sometimes even if you have a secure SSL/TLS connection. Speaking of that, before you submit any sensitive information to a Web site (i.e., from making a purchase or checking your bank statement), make sure that an encrypted link is in place. Make sure the lock icon is "locked" in your browser -- usually in the lower right corner of the window.

Step 4. Tools you can use to test if you're vulnerable

If you're even somewhat serious about securing your information, you can use various tools that show you what the bad guys see. Ideally, you should run these tools on a separate computer with a wireless connection. This will create a real-world environment and allow you to replicate an attacker's system looking in on your wireless laptop(s). Here are some tools you can use along with what they accomplish:

- Port scanners such as SuperScan and nmap to find out what's running on your wireless system -- it's the first step to breaking in.
- Vulnerability scanners such as NeWT, LanSpy, or LANguard to see what's easily exploitable.
- Network analyzers such as CommView for WiFi and AiroPeek to view cleartext information, where you're browsing, who you're talking to and more, all as it passes through thin air.
- A penetration application such as Metasploit to actually exploit the operating system and application vulnerabilities found. However, quite often all that's needed is a basic command prompt to establish null sessions, map drives, browse shares and more
- Password crackers such as Proactive Password Auditor, LC5, pwdump3, and NetBIOS Auditing Tool (NAT) crack your Windows passwords once that coveted remote connection is made.

Some of the bad guys have these tools, but odds are just as many -- if not more -- aren't as sophisticated. However, if you're like me, you don't want to take any chances. Perhaps it's time to lock those wireless laptops down a little tighter?

ABOUT THE AUTHOR:

Kevin Beaver

Kevin Beaver is an independent information security advisor with Atlanta-based Principle Logic LLC. He has more than 17 years of experience in IT and specializes in performing information security assessments. He has authored five information security-related books including *Hacking For Dummies (Wiley)*, *the brand new Hacking Wireless Networks For Dummies*, and *The Practical Guide to HIPAA Privacy and Security Compliance (Auerbach)*. You can reach Kevin Beaver at kbeaver@principlelogic.com.

Copyright 2005 TechTarget