STAR Watch

Statewide Technology Assistance Resources Project

A publication of the Western New York Law Center, Inc.

Volume 8 Issue 6 December 2004

How Safe is Your Wireless Network?

It wasn't that long ago that the only way to network computers was through hard-wired connections. That made security a simple issue. Network administrators were able to control access to the network by controlling the physical connections into the network. As wireless network hardware has gotten faster, more sophisticated and cheaper, it is becoming the standard way of networking in many offices. But that has led to security issues that could never occur in a hard-wired network. Many of the network administrators who have made the transition to wireless are unaware of the gaping holes in their network's security that await exploitation and how simple it is to secure a wireless network.

In order to make the installation of a wireless network simple, most manufacturers configure the equipment with all security features turned off. The assumption is that users will get the network up and running, then apply appropriate security features. Sadly, many users (and network administrators) consider the job to be complete as soon as the wireless connection works. If none of the security features are implemented, anyone with a computer and a wireless network card can jump onto your wireless network.

Because wireless networking is designed to be simple to install and easy to use, wireless devices don't automatically distinguish between an authorized user and an intruder—They must be told. Most wireless networking systems allow administrators to apply multiple layers of security:

1. All wireless routers/access points require a userid and password to access its settings and features. All devices fresh out of the box have the same factory-assigned userid and password. It's printed in the instruction manual. It's on the manufacturer's web site. Anybody can find out what it is. Change it! It will prevent unauthorized changes to functionality and security. This is the number 1 mistake made by neophytes.

2. Change the IP address of the router / access point. Just like userids and pass-

In this issue…

words, brand-new equipment is factory-set to a specific IP address. Anyone who knows anything about the brand of device used can find out the factory-assigned IP. It's much more difficult for an outsider to hijack a network device if the IP address is unknown.

3. Enable WEP encryption and use a non-obvious encryption key. Your initials or the initials of the organization are not good enough. When a computer attempts to connect to a wireless network, it must provide the correct key to the access point / router. If it is not correct, the computer is not allowed to connect into the network.

4. WEP encryption keys should be changed periodically. If an unwanted intruder was able to discover the WEP key in use, it would be useless to them after the key was changed.

5. Every wired and wireless network adaptor has a MAC address burned into it. While there is no guarantee that it is absolutely unique, it is "unique enough" to be used to identify computers that are attempting to log on to the network. Most wireless access points / routers can be configured to only communicate with machines that have specific MAC addresses.

6. Don't broadcast the existence of the wireless network. By their very design, wireless devices are constantly sending out signals called "probes" indicating that they are available and seeking to "hook up" with a nearby access point. In turn, every access point transmits "beacons" inviting probes to link up. Turn off the SSID broadcast feature on the access point / router.

But there is no wireless network here…

You don't have a wireless network, so none of these admonitions apply, right? Maybe not. Maybe there are wireless networks attached to your hard-wired network—you just aren't aware of them. There are published articles about employees bringing in their own notebook computers from home. In order to move files to their notebook computer, they connected an inexpensive access point to an available data jack in the hard-wired network. When they left work for the day, the access point remained connected to the network and powered up. No security features were enabled. Reports vary on the amount of damage done by hackers.

In another account about a large corporation, auditors brought in and installed a wireless router in a conference room so they could all be online. That inadvertently put sensitive financial information out in the air.

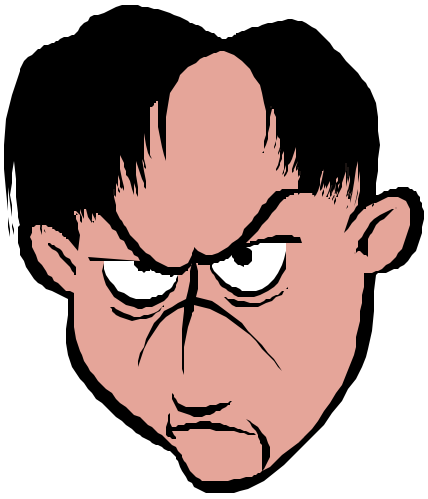
. . . . .

Wireless networking is a great technology that can provide a reasonable level of security when properly configured. Wireless networks are usually most vulnerable at initial installation when network administrators are not aware of all that should be done to safeguard the network from unwanted intrusion or have been hurried into installations without the proper amount of preparation time. Any security risk created by a wireless network can be neutralized with adequate planning and attention to detail.

Life After Windows XP Service Pack 2: Reclaiming Performance

Are you experiencing a loss of performance? (No, this is not about any of those products that we all have received as spam.)

In a sadly misguided effort to protect computer users from themselves, Microsoft includes the Internet Connection Firewall in all versions of Windows XP. According to Microsoft, "Internet Connection Firewall is software that you can use to set restrictions on the information that is communicated between your home or small office network and the Internet. It is a good idea to turn on Internet Connection Firewall on the Internet connection on any Microsoft Windows XP-based computer that is connected directly to the Internet. If you have a single computer that is connected to the Internet with a cable modem, a DSL modem, or a dial-up modem, Internet Connection Firewall helps protect your Internet connection".



They say that it is a good idea to use it and it's provided at no cost—monetary cost, that is. Performance cost is something completely different.

A while ago, we purchased a shiny new computer with Windows XP Professional installed on it. Instead of scrapping the old computer, we networked both computers so that either computer could access the Internet. When Service Pack 2 for Windows XP was announced, we dutifully installed it. It was then that we noticed 2 big issues:

1. When the older computer was used to download large files from the Internet, the download speed was approximately 10 times faster than downloads on the brand-new, super-fast machine.
2. Copying files from one machine to the other became painfully slow. When attempting to copy very large video capture files, Windows Explorer would estimate the time to complete the copy in hours. It would have been faster to re-capture the data from the original video.

The Internet Connection Firewall was a suspect immediately (we have learned to be suspicious of new functionality—especially when it's provided at no additional cost from Microsoft), but simply turning it off from the system tray (in the lower-left corner of the screen) did not have any noticeable effect. It was the same story when we attempted to make changes to any of its configuration settings. We performed all of the steps outlined in the Microsoft KnowledgeBase article 305549 ("How to configure a connection to the Internet in Windows XP Professional"). It didn't help. So then we followed the steps in KnowledgeBase article 283673 titled "HOW TO: Enable or Disable Internet Connection Firewall in Windows XP". That also did nothing to help.

After a little more perseverance, we struck gold. KnowledgeBase article 886264 ("Programs that may experience a change in behavior after you install Windows XP Service Pack 2") contained a laundry list of well-known computer applications and "issues" that could arise after installing Service Pack 2. The issues ranged from minor annoyances, to applications that stopped working completely. (Yes, there were many applications from Microsoft that were affected). Most solutions were reasonably simple to implement for any computer-literate user, although a single workstation running Windows XP Service Pack 2 might require dozens of these "solutions". Other solutions might require a techie to accomplish.

Stepping back and looking at the bigger picture, we were struck by the large percentage of issues that involved one specific product: Internet Connection Firewall. Our suspicions about possible culprits appeared to be confirmed. Could it be that this piece of software causes more problems than it allegedly protects us from? Oh please Mr. Gates, say it isn't so!

After about 3 nanoseconds of soul searching, we decided that Internet Connection Firewall must be eradicated. It took a little more research, but finally, we located the information we sought. Another article in the KnowledgeBase, 842264 ("Network performance and data throughput may be significantly slower after installing Windows XP Service Pack 2"), we learned that the phrase "disabling the Internet Connection Firewall" has a different meaning depending on which article it is contained in. All of the previous procedures that we followed stopped the firewall from any filtering activity, but it was still running in the computer system, but letting everything pass through—after a signifi-

cant amount of time had passed. This article also explained how to totally remove the Internet Connection Firewall from the computer:

1. Go to **Start** > **RUN...**
2. Type in **SERVICES.MSC**; The **Services** screen will be displayed.
3. In the right-hand panel of the screen, near the bottom of the list, right-click on **Windows Firewall/Internet Connection Sharing (ICS)**, and then select **Properties**
4. On the **General** tab of the screen that is displayed, change **Startup type:** to **Disabled**
5. Click **Apply** at the bottom of the screen
6. Then, under **Service status:**, click **Stop**.

Now, the Internet Connection Firewall is truly gone. It will not be loaded at computer startup. It can no longer strangle downloads and/or file copies.

The Results...

The Windows XP machine could now download files as quickly as the old Windows 2000 computer. Copying files from one computer to the other speeded up tremendously. Thank you, Mr. Gates for this fun experience.

But what if you really need a firewall?

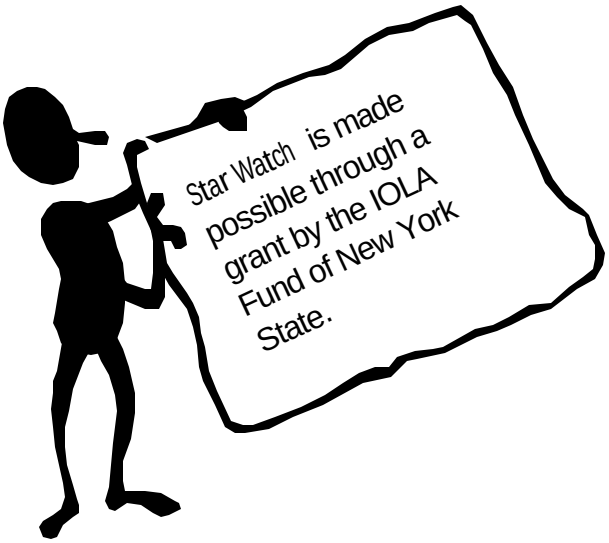
If the computer that you are concerned about shares its connection to the Internet with other computers, it is probably protected by a firewall already. The firewall is in the router that connects the local network to the Internet connection. At home, it is a different story. Most home users have a single computer connected directly to a dialup, DSL, or cable modem. Probably, there is no firewall to keep out unwanted pests when connected to the Internet.

Several reputable companies have marketed personal firewall software at an average cost of $10-$40. But why spend the money when there are good products available for free? ZoneLabs allows free downloads of Zone Alarm, its personal firewall. To get a copy of this free software, go to: http://www.zonelabs.com/store/content/catalog/products/sku_list_za.jsp and click the **Free Download** button.

WNYLC Web Statistics For November 2004

Total Hits……318,989
Total User Sessions……..36,809
Average Hits/Day
(Monday – Friday)……13,321
Average user Sessions/Weekday…..1,466
Number of Pages Viewed……102,757
Average Number of Pages
Viewed Per Day……..……3,425
Number of Documents Viewed…….69,447

Accessed Using Internet Explorer…….90%
Accessed Using Netscape……..……4%
Operating Systems Used:
Windows 98……..……..24%
Windows 2000……...……..24%
Windows XP……..……...40%
Windows 95……...……<1%
Windows ME……...……1%
Windows NT……..1%
Macintosh……..…<1%
Linux/Unix……...<1%



WHO WE ARE

Joe Kelemen - Attorney
Kathleen Lynch - Attorney
Tom Karkau - Programmer
Carly Bouchard - Administrative Assistant

Wnylc@wnylc.com

716-855-0203

www.wnylc.net

Western New York Law Center, Inc.
237 Main Street, Suite 1030
Buffalo, New York 14203