HOME NETWORK SECURITY/FIREWALLS

Introduction

If you do not take reasonable actions to secure your home network, you are putting yourself and others at risk. As with any risk assessment, you can think about it in terms of the likelihood something will occur and the consequences. It's unlikely that you and your home network will be targets of anything. But it's very possible. Computers connected to a network are vulnerable to being sensed by others. The bad guys can use things called "port scanners" or similar technologies to swipe across large swatches of computer addresses that maybe connected to the Internet. But I am talking about YOU in particular. You are probably going to be just fine. Unfortunately, this is one of those "Someone only has to get in once and you will be very, very sorry" kind of thing. The compromise of your home network not only offers someone access to your personal files, but offers up your computer as a resource. Using your system's computing power and network connection, someone in control of your computer could launch attacks against other computers or whole networks. And your system will be part of a long trail attempting to conceal where such an attack originated. By protecting your home network, you are doing something similar to having a car alarm and other anti-theft devices installed. You eliminate a broad range of low-skilled opportunistic thieves who will just move to an easier target.

For most typical home users slogging through the Action steps below is not fun. Not everyone wants to become proficient at home networking. Most everyone just wants to use the Internet at high speed and not be bothered. Thankfully, you really only have to go through all of this once. (However, it's not a bad idea to review your home network security every so often.) Once you're done, you'll have a high degree of confidence that you're reasonably safe. You have to take these steps though.

There is not a high enough general awareness that home network security is important to overall network security. Be sure to tell your

family and friends that they too could be at risk and that they need to take some protective action.

Taking Action

Secure Your Home Network

If you use a traditional modem to dial into the Internet, you will not be faced with nearly as many problems. Neither will you have the benefit of the newest high speed connectivity. If you are concerned with home networking security, it's more likely you have purchased high speed service and this comes into your home via Cable or Digital Subscriber Line (DSL) technology. In either case, you have a cable coming from your computer's networking connection going into a box, that in turn has a cable going into your wall. If you are hooking up multiple computers to your connection, you may have a router, wireless or otherwise, hooked up between your Cable/DSL box and your computer(s).

If you are not using a router, you can skip the Router section just below and read up on Firewall Technology. If you are not using a router device (which can serve a hardware type of firewall protection), you will need to get some software firewall protection to keep the bad stuff out.

Routers

If you have purchased a late model router, the setup instructions should include most of the following information. Older routers may have shipped with instruction manuals that did not emphasize any need to re-configure things from the default settings. In fact, you do not really have to do so in order to make things work. However, this is a risky thing to do. The default settings for routers, most especially wireless routers, are well-known. Leaving the default settings is similar to leaving a key to your home hanging from a nail in your door. (Not even under the front mat.)

Routers can seem complicated. The setup screens may have a lot of cryptic acronyms, wording and numbers, such as IP addresses. Most of this you do not need to have deep knowledge about. It cannot hurt to learn more about the technology; however, it's not really necessary. All you have to really know is that an Internet Protocol (IP) address

is just a way of identifying a particular computer. Your home address isn't complicated. It is something like 123 Main Street. Think about longitude and latitude. You probably know what this is, a string of numbers representing a location on the earth somewhere. It could look like this, 41.118N -73.955W. You are not likely to use such a thing on a daily basis, even if your new car GPS system does. And maybe it is a complicated way to navigate around. But you understand what it is easily enough. IP addresses are the same way. Do not be intimidated by the way the numbers seem to look. It's just an address.

It may be helpful to know that there will be a WAN address associated with your router. (That's a Wide Area Network address.) So when you plug everything in and set everything up the way your manuals say to, your service provider should automatically provide an address to your router. You might not ever even see this address. Then your router assigns different addresses for each of your computers. Information just passes from one to the other the same way that you have all the cables wired up. (With a bit of a jump through the air if you are using wireless technology.) In any case, the risk is that somewhere out there, before the wiring makes it to your house, someone is hooked up and looking for your address. Ideally, an address where someone has left a door open. When they find it, they want to come in. Following are some methods to shut and lock the doors.

Router Setup

- Check your router manual and follow the instructions to access your setup screens. Then follow the instructions below.
- Change the SSID. This is the "Service Set Identifier" for your Wireless Access Point (WAP). The SSID is what makes your network different from others. In fact, if you live in a condo or apartment building and do not change this, you may be sharing more than a building with your neighbors very quickly. See the "Password" section for help in choosing a good password for this. Someone making it through here could gain access to any computer on your home network. And they may be able to do so with a laptop in a car across the street.
- Turn off SSID Broadcasting. Think of this as having an unlisted phone number. Or at least, not shouting out to other wireless computers, "Hey, there is a connection over here!!!"

Change the setting to "Disabled" or "Closed Network." The terminology will vary per vendor.

- You can use Media Access Control (MAC) address filtering to allow only known hardware devices access to the router. That is, the computers you have in your home as opposed to the wireless laptop your neighbor has. Your network cards each have their own address. You'll need to remember you did this if you add other devices to your home network. (You'll probably remember if you do add things and you cannot get them to work.) To use this, you'll need to determine the Network Adapter Addresses for your devices.
  - ◆ Windows: There are actually multiple ways to get this information, but the fastest is…
  - ◆ Select Start > Run
  - ◆ In the window box, type "cmd" then press [Enter]
  - ◆ An older style DOS window will show up.
  - ◆ Type "ipconfig /all" and press [Enter]
  - ◆ Look for the line on the screen that says "Physical Address" and write this long number down. This is the MAC address in what is called hexadecimal format.
  - ◆ You will need to follow the instructions for you router to enter this number into the MAC setup for your router.
- Remote Management should be set to Disable or Off. Unless you really know what you're doing, this should be set to Disable.
- If you would like additional protection, set up and enable the Wired Equivalent Privacy (WEP) feature. This will encrypt wireless data. Even someone somehow receiving the transmission will not be able to decipher your message traffic. This is something you may need to remember if you use Wireless Access Points in multiple locations via a laptop. Your laptop wireless card software will ideally have the ability to set up multiple configurations. If not, you'll have to just turn WEP off or on as desired. Or choose not to use it at all.
- Investigate other security features. Some vendors may have additional parental controls or other advanced features.

Use Firewall Technology

As the name implies, Firewall technology is built to put up a wall disallowing unwelcome things from entering your computing environment. Firewalls analyze the message traffic going back and forth between your computer, your router and the Internet connection. They have the ability to detect various forms of unauthorized traffic. A full technical discussion is beyond the scope of this book. Several Internet resources are listed below if you would like to research this further. The key thing for you to understand is that having a Firewall is a key part of your home or small office network security.

If you are using a router, it should include hardware based firewall security. Even if you only use one computer at home and do not need a router, you can still get one to place between your computer and your cable or DSL modem for added protection. Think about it this way: You could have an amazingly effective team of bouncers at your party, but if you never let the troublemakers in the door, that is still less of a problem. While software based firewalls running on a PC can be effective, they can possibly degrade system performance more than a dedicated piece of hardware would. If you're using modem dial-up, you'll have to opt for software based protection. (Fortunately, dial-up users are less likely to be attacked than "always on" connections.)

Firewall technology can help protect against several forms of attack. Distributed Denial of Service (or DDos) is one of the more common. The way it works is that a hacker makes his way to your computer via a number of different network "hops" trying to cover his tracks as he goes. Your computer may be an actual target, receiving so much messaging traffic your equipment cannot handle it. But more likely, the target is a more public system. You're getting set up as the one that is doing the attacking. But just how will your computer be attacking? The hacker will have a program running on your computer. He'll have this because you didn't take adequate precautions to stop him. The program will attempt to flood the Internet or a particular target site with various kinds of message traffic. The goal is to flood the target to the degree that the target's Internet connection and perhaps their computers are unusable. This may make the evening news. Or the world news. It depends on a) was the attack somewhat successful and b) was the attack some kind of funny prank? Or did you just help shut down a hospital or military station or power plant? So, your computer

may be one of many enlisted in such an attack. And the attacking program may also be spreading virus-like copies of itself to others to press the attack further. (Such viruses are also known as worms or Trojan Horses.) The hacker could have set this up days, weeks, even months prior to the attack, which could be kicked off based on your computer's date setting or other means. You could even be away for the weekend while your computer participates in a worldwide network attack. You have a responsibility to not make this an easy thing for others to do. By just protecting your own home network, you make it a little harder for the those who would launch network attacks.

A more specific attack might use "spoofing." Spoofing is a means by which a hacker pretends to be a friendly web site or Email server or other Internet service. More broadly, the hacker makes your computer think the traffic it is receiving is from a known, trusted source. From there, your data can possibly be captured.

Firewall technology can reduce or eliminate these and other risks. Relative to the cost of entire systems and monthly costs for service, the additional cost is well worth the benefit. Hardware can be had for well under $100 and well known software in the $30 - $60 range. There is little excuse to not take these precautions.

Keep Your Software Updated

- Operating System Software must be kept up to date. Allow for automatic updating of your system software.
- Virus software must be continually updated. You should only use virus software products from established, reputable vendors that offer constantly updated subscription services. Several well-known vendors are listed below in the Additional Resources section.
- Firewall software must be updated. If you do not have automatic updating capability for your firewall software, keep up with any Email notifications informing you of updates. Otherwise, check back with the vendor web site on occasion.
- Router firewall software also should be checked for currency on occasion. Though less frequent than software updates, router companies do occasionally upgrade the "firmware" in their devices. It's often possible to download an update program which will upgrade a hardware device such as a router.

Beyond the Basics

There are many software services available on your computer that you're probably not even aware of and that you don't use. Software manufacturers and computer companies may be distributing systems to you that have certain services available by default. This is done with assumptions regarding what people are likely to use. Some of these services may be of sorts that have communications capability. For example, to provide web or file transfer services. While you may enjoy using your web browser, most people do not have a need to have a web server running. You may or may not have some of these extra, non-essential services active on your computer as it was shipped to you.

If you are using a home network, you will be using some of these more advanced features. But if not, you don't really need these features and should consider turning them off. They don't necessarily represent severe risks if taking the general precautions any responsible home network user should. However, anything you really don't need which represents even the possibility of a risk might just as well be removed. If you strongly anticipate needing them in the near future, you may leave these services intact.

Windows File & Print Sharing

- File Sharing can be found in Windows XP Pro and 2000 systems via the Start Menu. You may also be able to find the file sharing controls by right-clicking on "Network Neighborhood" if you have that icon on your desktop. Otherwise…
- Choose Control Panel
- then Network Connections
- then Local Area Connections
- Choose Properties
- If File and Printer Sharing is checked, uncheck it.
- Select 'OK'
- You will likely have to re-start your computer for these setting to take effect.
  - ◆ Windows XP Home edition does not support password protected file sharing. As a result, follow the directions above, however instead of properties, you may wish to choose "Uninstall" for the File and Printer Sharing option.

◆   For older Windows versions, you must also go through the Control Panel to get to the Network Settings area to unclick (if necessary) any entries for File and Printer Sharing.

Note: You may need to be especially careful with things like file and print sharing if you use a cable modem. By nature of how cable companies have set up cable modem networks, you may be just one of many network nodes within one single network. Your neighbors may be thought of as being on your own local area network. Try opening your "Network Neighborhood" icon, or use Start > My Network Places to see if you can see any other computers. If you can see them, they can see you. This may not be a big deal and your computer may not be at risk. But you must be more careful about things like File and Print sharing. You may also want to re-check what the name of your computer is. If it's your own name, or something that could identify the unit as belonging to you, you may want to change it to something more obscure.

Before you do this, you should know that renaming a computer may require that you go to another workgroup computer to change security permissions allowing the new computer name access to network resources. Such networking topics are beyond the scope of this book. If you have a full network setup, it's likely you are already aware of how to perform these tasks. If not, you may want to hold off on doing this until you can find network knowledgeable assistance.

In Windows, this will be available to you somewhere from Start > Control Panel. Select the "System" program to launch a dialog box and click on the Computer Name tab. You will have the means to change the computer name here. You will probably have to restart your computer after doing so. Renaming a computer is not a big deal. However, there could be an issue if you have multiple computers set up in a home network or workgroup.

Windows IIS Web Server

This work is primarily oriented towards home users not likely to be using these operating systems. Refer to your documentation for details if you are running these systems and wish to remove them. Or visit this link for more information…

Duke University Security Site

security.duke.edu/windows/disable_iis.html

Microsoft Messenger

Messenger may not be something you even know about. It's a means by which a network administrator can have a small alert box pop up on your screen. If you're on a network at work, you may have seen this. It might have said something like, "4th floor printer will be unavailable from 4pm – 6pm" or something similar. You should not get messages via this means, however, it's conceivable this could present a security hole at some point. If you don't use it and you don't need it, shut it off. This is only of concern to late model Windows users. Windows 9x and ME will not be affected.)

- From the Start Menu
- RIGHT-click My Computer.
  - You might not use this much. It's below the My Documents, My Pictures, etc.
- Select Manage
- Click the "+" sign next to Services and Applications. (Or just double-click Services and Applications.)
- In the right panel now, scroll down to Messenger. You can just type letter "m" to fast forward down the list.
- Double-click on Messenger.
- Select Stop from the properties window.
- Change the Startup type: to "Disabled"
- Click 'OK' then close the Computer Management window.

For Macintosh

For Pre OS X systems… (OS X is not a problem as they wisely have decided to ship with sharing disabled.)

- Go to the Sharing Setup Control Panel
- Both the File Sharing Button and Program Linking Button should be set to "Stopped." In other words, if the button says "Start" that means it's currently set to Stop, which is fine.

Additional Resources

Home Network Security

CERT® Coordination Center
www.cert.org/tech_tips/home_networks.html
Help for Home Network Security
www.cert.org/tech_tips
Tech Tips
Firewall Software Reviews
from Steve Gibson, Gibson Research Corporation
grc.com/lt/scoreboard.htm
Gibson Research Corporation
Easy to understand explanation of how firewalls work. Includes online tests to see if your network is secure.
grc.com/su-firewalls.htm
Home PC Firewall Guide
www.firewallguide.com
Microsoft
How to Protect Your Network
www.microsoft.com/WindowsXP/pro/using/howto/networking/homenet/protect.asp
tech tv
    Several great articles on firewalls. Unfortunately, their web site is setup that deep down articles have very long web addresses. Go to the site's front page, type "firewall" in the search box, set the date back at least 6 months and initiate the search.
    www.techtv.com

Home Network Security Testing
HackerWhacker: www.hackerwhacker.com
Broadband Reports: www.dslreports.com/secureme
NetStumbler for Wireless: www.netstumbler.com
Shields UP!!!: www.grc.com
Symantec Security Scan: security.norton.com

Equipment Vendors (Routers, Firewalls)
D-Link: www.d-link.com
Linksys/Cisco: www.linksys.com
NETGEAR: www.netgear.com

US Robotics: www.usrobotics.com

Software Vendors

All of the software vendors below are well-known brands within the Firewall category. All have well-known products which have been on the marketplace for some time. Visit their sites to compare features. The feature comparison alone is an excellent education helping you to decide what protection issues you are most concerned with.
BlackIce
from Internet Security Systems. Intrusion detection and personal firewall.
www.iss.net/solutions/home_office
IPSentry
Network monitoring software..
www.ipsentry.net
McAfee Firewall
Several stand-alone and bundled offerings from a leading virus and security software vendor.
www.mcafee.com
Microsoft XP Firewall
Instructions on how to use the built in Internet Connection Firewall to secure your home or office network. This software is already installed with Microsoft XP.
www.microsoft.com/windowsxp/pro/using/howto/networking/icf.asp
Sygate Personal Firewall Pro
Firewall protection and intruder tracking tools.
smb.sygate.com/products/pspf/pspf_ov.htm
Symantec
Personal Firewall and privacy protection.
www.symantec.com/sabu/nis/npf
zeroknowledge systems
Freedom firewall and internet security.
www.freedom.net/products/firewall/index.html
ZoneAlarm
Firewall protection, hacker tracking, advisories.
www.zonelabs.com