Global Information Assurance Certification Paper

Understanding & Securing Home Windows Networks

Todd Grigsby

GSEC Practical Version 1.3

January 23, 2002

Introduction

My goal is to present home computing novices a white paper to understanding today's Internet Service Providers (ISP) offerings and methods to which you can secure your home Microsoft windows networking environment as effective as possible. Lets clearly understand that there isn't anyway to completely secure any environment from all hackers, unless you have the resources to secure your network as tightly as the Pentagon's classified network is reported to be. Obviously I not attempting to say that any home network will ever be as secure as the Pentagon's classified networks but I am going point out methods, that, if followed will provide your home network with a more secured environment than it would be straight out-of-the-box as most home networks are setup and maintained today.

Over the last few years home networking has become much more common place with the desire for households to share information and resources amongst other family members as if they were in an office environment. Kids using computers have become savvier, in some cases, than most of the adults using computers and networks at home due to the fact that they simply use them more often and learn quicker than many adults. Most home computers are used for what now seems to be typical daily activities such as Internet access, e-mail, checkbook accounting, bill paying, schoolwork, research, etc. Now, along with Internet access comes a multitude of security threats through activities which, typically includes downloading of information/data (mp3 music, documents, pictures, applications, program updates, etc.), online purchasing which, of course includes the transferring of your credit card information just to name a few potential security risk points. With the downward trend in the cost of computers, home networking equipment and ISP access more and more households are taking advantage of high-speed access to support their ever-expanding needs for more bandwidth.

Types of Network Access

Today's ISP's offer a variety of available access methods and speeds for home networking users. As prevalent as cable modem and Digital Subscriber Line (DSL) broadband high-speed access is, dial-up access by far supports the largest number of home networking users nationwide. Provided below is a brief discussion to assist novice computing users the benefits in understanding each technology.

1. **Dial-up networking**.

   The easiest form of access and quickest to obtain is dial-up networking. The most well known ISP is America On-Line (AOL) supporting over 20 million users. Most current dial-up modem connections support bandwidth speeds up to 56 kbps (kilobits per second or thousand bits per second). Dial-up speed depends on your computer's modem and the ISP's modem speed. Both modems at each end of the dial-up connection must support the same level of speed, 56 kbps, in order to obtain that speed. For instance, if your modem supports 24 kbps and your ISP supports 56 kbps than the highest speed of your connection will be 24 kbps. Your lower speed modem cannot support the algorithm and data compression capabilities of the higher 56 kbps modem thus the higher speed modem will negotiate a data transfer speed that both modems can support.

2. **Broadband networking**.

   Broadband networking is commonly referred to as high-speed network connectivity. ISP's, which support high-speed networking, provide cable modem and DSL Internet access to home users. ISP's such as Comcast cable and Verizon support high-speed cable modem and DSL access respectively. Bandwidth is the term used to describe the speed of a network connection. For broadband, there is no set minimum speed that determines what a broadband connection is, but typical broadband connections run in excess of one megabit per second (Mbps).

   a. **Cable modem access**.

      Cable modem access is provided by your neighborhood cable TV provider and usually has an Ethernet local area network (LAN) connection to the computer, and is capable of speeds from 1 to 10 Mbps. Typical access speeds tend to be lower and speaking from personal experience with my own cable modem access usually runs at about one Mbps. Cable modem providers will boast about higher maximum speeds, but since cable providers turn entire neighborhoods into LANs, which share the same bandwidth thus reducing your network access speed as more and more users come online. Nevertheless, given the speed increase over 56 kbps and the capability of supporting multiple users within a single home at the same time with a low priced network hub make cable modem access very attractive. Cable modem users may also be susceptible to risks such as packet sniffing since entire neighborhoods of cable modem users are effectively part of the same "neighborhood" LAN. Any cable modem user's computer in a neighborhood setup with packet sniffing capability may be able to capture data transmitted by any other cable modem in the same neighborhood LAN. Data encryption can help

protect your important data from most packet sniffers. Encrypting your data isn't necessary between secured web sites, which is discussed below in the Web Spoofing section. If you are very concerned about the content of your data and e-mails between your computer and associates and friends, then you should consider the use of encryption, which is discussed below in the Encrypting Your Data section.

b. **DSL access**.

Digital Subscriber Line (DSL) access provides household users with dedicated Internet connectivity. Typically, DSL bandwidth ranges from 144 kbps to one mbps or higher but your speed depends on the distance from your house to your nearest telephone company central office (CO). Unfortunately for most home users DSL is not a viable option since the maximum distance from your house to a CO is approximately 18,000 feet depending on the DSL providers limitations. Most homes tend to be further away from the CO. When DSL speaks of dedicated bandwidth, that bandwidth is only dedicated from your house to the telephone company central office. Once it leaves the central office your bandwidth becomes shared at that point with other Internet traffic. DSL is priced a bit more toward the business user end. Typically, based on my research on Verizon and Covad DSL and Comcast and Adelphia cable modem pricing, DSL runs at approximately three to five times the price of cable modem access.

3. **Dial-up versus broadband services**.

One of the positive aspects of dial-up Internet access is the fact that it is considered on-demand service. Meaning that you're connected to the Internet only while you need it and that you typically disconnect after your work is completed. Another key aspect of dial-up access is that you dial into a pool of modems at your ISP. A feature of modem pools is that IP addresses are dynamically assigned to each connection. Simply put, each time you connect to your ISP your computer is usually assigned a different IP address, which makes it much more difficult for a hacker to take control of your computer.

Everything connected to the Internet is assigned an IP address. Think of an IP address as a unique identifying number assigned to your computer so that when you're exchanging information between you and a web site, the web site knows where you are in the vast Internet world. Your unique IP address is the method at which you are identified among the masses. You can also think of IP addressing as a telephone number. Every telephone in the world has a unique telephone number assigned to it, correct? IP addresses act like telephone numbers except that they arranged in four groups with up to three numbers per group and separated by a period, or dot in IP ease. An

example is 170.109.2.34. Your computer may have 64.127.111.2 and it can change every time you dial into your ISP's modem pool.

Broadband services are considered as always-on services because there is no dialing to setup your connection. Your network connection is always there ready for you to access the Internet whenever you're ready. This also means than even though you may not be surfing the Internet, if your computer is on and your network interface card (NIC) drivers are loaded (which typically are loaded at startup) then your computer is continuously connected to the Internet. While dial-up IP addresses are dynamically assigned at each connection, broadband IP addresses are typically assigned at cable and DSL modem startup or boot time. Cable and DSL modem startups typically occur much more infrequently if your service is stable and available. This means that your IP addresses change less frequently and are more prone for hackers to figure them out and gain control of your computer.

Types of Attacks

There are many types of cyber attacks that are well documented and many that are not. Below are a few of the better known cyber attacks and cyber acronyms to provide home users with a basic understanding of what can possibly occur to your home computer.

Hacker – A person who gains unauthorized access to computer systems in order to destroy, steal or alter data, or to launch attacks from one computer to other computers for devious and unlawful reasons.

Web Site Defacement – Changing a web site's information without the owner's written permission. This can be extremely embarrassing to an owner if this is a company web site since the "redecorating" of a web site may depend on the maturity level of the hacker. This can range from obscene gestures and verbal attacks, racial slurs, inserting hyperlinks to other web sites or simple changes background colors. The key issue is that you did not authorize any of these changes and you certainly do not want to be associated with these modifications.

Denial of Service (DoS) – The idea of a denial of service attack is to prevent you from using your computer system by keeping your system so busy with thousands of information requests that your computer or web site cannot service any other request for legitimate information. A DoS attack could also prevent customers from accessing an e-commerce web site such as amazon.com during the Christmas season or a financial web site such as E-trade.com during stock trading hours. Obviously this would cause a business to potentially loose hundreds of thousands of dollars depending on amount of downtime. Downtime is not exactly the correct term to use when describing a DoS attack. A DoS

attack actually involves the deliberate prevention of allowing anyone access to a web site or your computer. Your data is typically still intact but access to your computer or a web site is not available until the DoS attack is stopped.

Distributed Denial of Service (DDoS) – In my opinion this is one of the more likely attacks on your computer since it hides the identity of the hacker but unfortunately identifies "you" as the initiator of the denial of service attack. This is another form of denial of service but is typically more widespread in that it involves multiple computers, from potentially around the world, attacking a web site and thus is a distributed attack from across the Internet. The hacker will hack into your computer and launch a program from your computer that will initiate a denial of service attack against their ultimate target, which is typically a company web site. In this situation the hacker has also hacked into other computers across the Internet to perform the same function as your computer is performing for the hacker. The hacker doesn't have to physically hack into your computer at the time of the DDoS. The hacker may have attacked you at an earlier time and left a worm (virus) program to launch at a specific time to perform its malicious deeds. If you sometimes leave your computer on all night long this worm could launch at midnight and if you're on a cable modem connection, run its DDoS for a few hours and stop. By the next morning you may have no knowledge of what happened the night before.

Web Spoofing – Web spoofing allows a hacker to intercept data being sent from your computer to a trusted web site or remote user. Once intercepted, the hacker can then pretend to be the trusted remote end and send messages back to your computer making it look as if you're still communicating with your trusted destination. In other words, the hacker is tricking, or spoofing you into thinking that you're still exchanging information between your computer and the remote web site. This interception of information may be e-mail messages or a credit card number you're using to purchase something.

Please understand this is *not* easy for a hacker to accomplish especially when it comes to credit card information when almost all e-commerce web sites use SSL (Secure Socket Layer) encryption. You'll be able to tell if you are entering a secured web server by either a popup window telling you you're entering a secure web site, your web browser will display a lock on the lower bar, or your web site address line will read "http**s**://" to illustrate that you're on a secured web server. SSL allows you to securely send data without it being viewed as regular text. Instead your text is garbled into random characters being sent from your computer to the remote web server. Both your computer and the remote server have negotiated keys to reassembled the data back into readable data. The negotiated keys are randomly created by use of a complex algorithm and are extremely difficult to break.

Types of Home Network Security & Prevention Methods

There are many types of home network security and prevention methods that are effective, inexpensive, comprehensive, and easy to use for the general home user. They range from personal firewalls, anti-virus software, performing patch updates by checking Microsoft's web site for operating and application software updates, and checking informational web sites for general updates on malicious attacks and general computing information including, but not limited to.

- www.cert.org - The CERT Coordination Center (CERT/CC) is a center of Internet security expertise operated by Carnegie Mellon University. The site is typically for more experienced computer users but contains a wealth of information that is constantly updated on Internet security vulnerabilities, computer security incidents, security alerts, research long-term changes in networked systems, and develop information and training to help you improve security at your site, including your home.

- www.microsoft.com - Microsoft Corporation web site provides numerous informational updates on their own as well as other security issues within computer and networking environments. Current issues for Microsoft centers on Windows XP security breaches within XP's universal plug and play capability. Microsoft also provides other updates as well as general information on all Microsoft products.

- www.sans.org - The SANS (System Administration, Networking and Security) Institute is a cooperative research and education organization of security professionals, system administrators, and networking professionals providing an amazing wealth of information that is hard to surpass. The information ranges from highly technical "white papers" to information that entry-level novices can easily understand.

1. **Firewalls** - A firewall protects a computer network from unauthorized access. A firewall is considered the first line of defense in protecting private information. Firewalls may be hardware devices, software programs, or a combination of the two. A firewall typically guards an internal network against malicious access from the outside (Internet); however, firewalls may also be configured to limit access to the outside from internal users. Home users face the same security challenges that many corporations do. That is, they may be on somebody's hit list. While attackers may not specifically target your insignificant home computer, they know how easy it is to use an unsecured remote account as a jumping off point into someone's corporate network. The growing use of cable modems and DSL make home users an even more tempting target for hackers to utilize your computer in initiating cyber crimes such as denial of service (DoS), distributed denial of service (DDoS), web spoofing and web site defacement. For these and many other

reasons, home computers need firewall protection as much as the corporate network. The concept of a personal firewall isn't new. The first commercial software and hardware firewalls for personal computing and the home office hit the market several years ago. Today, if your company issues laptops for business use, changes are they installed software firewalls on these laptops as a matter of company security policy.

Personal firewalls are inexpensive, some are free, easy to install, fairly easy to operate and maintain. Many include a license to allow you to install a one-time purchase on multiple home-base machines making this a no-brainer for you to purchase and install a personal firewall on your home computers.

Here are a few of the top personal firewalls available today.

- Zone Alarm Pro 2.6 – www.zonelabs.com
- Tiny Personal Firewall 2.0 – www.tinysoftware.com
- Norton Personal Firewall – www.symantec.com
- Sygate Personal Firewall – www.sygate.com
- McAfee.com Personal Firewall – www.mcafee.com

An excellent resource to assist you in selecting and understanding more about personal firewalls and is free by connecting to the following web site. http://grc.com/lt/scoreboard.htm. This is Steve Gibson's (a noted expert on hacking and computer security) web site, Gibson Research Corporation (GRC). GRC also provides free personal firewall testing software as well as free personal firewall software that can be downloaded for evaluation. GRC's LeakTest firewall testing software is easy to use to evaluate your personal firewall selection, installation and configuration.

2. **Anti-Virus Software Protection**

Probably one of the most important aspects to computer/network security is installing anti-virus software onto each and every computer you own. One of the most effective ways for hackers to launch their attacks is by infecting your system with a virus. Viruses can get into your computer through multiple methods including the following.

- E-mail
- Removable media (floppy, Jaz Drive, Zip Drive, Tapes, etc)

- Internet downloads

For an attacker, e-mails are one of the easiest ways to get viruses to the masses. The “I Love You” and “Melissa” viruses were amazingly successful in that they were propagated by users simply opening an e-mail and double-clicking on the attachment without realizing what the contents were. The scary part is that it is so easy for someone to mistake e-mails containing a virus from a legitimate e-mail. The e-mail may come from someone who has e-mail you in the past, which could be either a friend or an associated. The e-mail will look normal, typically with a text message and an attachment. You should also never send or open programs via email, including files that end in suffix EXE, VBS, BAT, etc. These are executable files that could either be legitimate programs or viruses. It’s highly recommend that you do not open any attachment with these types of file extensions unless you are expecting this e-mail and attachment from a trusted source.

In the case of the “I Love You” virus, once you opened the e-mail and launched (double-clicked) the attached file then the virus took over your machine by constantly sending e-mails from you to your e-mail directory of recipients, which could range from a handful to hundreds of people. It would also infect .jpg (picture) files to act as .vbs scripts to perform again the just referred e-mail mass mailing routine if you opened your .jpg file at a later date. Essentially, you just lost all of your .jpg files permanently unless you have a backup of them. This is the virus replicating itself throughout your computer system. If this occurred to you at your office, the virus utilized your company e-mail directories as a resource for propagating itself to potentially thousands of people. Once one of your recipients opened the e-mail and attachment it would attack their system and propagate throughout their e-mail lists sending the e-mail and virus back to you as well. You can see how malicious and devastating that would be to not only your computer but to hundreds of e-mail servers throughout the world.

It’s actually very easy to understand what a virus is. It’s simply a computer program designed to cause havoc and inflict pain on anyone they infect. A virus’ game plan varies from the above stated e-mail propagation, file (jpg) infection, crashing your computer, erasing files or just making your computer run slower.

Additionally, if you are using Microsoft Outlook or Outlook Express make sure you are not using the preview pane viewer. With the preview pane in effect this can automatically launch the attached virus before you even have a chance to not open it. Turning off the preview pane is sometimes difficult to do. To turn off the preview pane in Outlook Express perform the following.

I. On the **View** menu, click **Layout**.

II. In the **Preview Pane** area, select the options you want and then click **OK**.

Here's the big question. What can you do to protect yourself from a potential attack? Fortunately, most all new computers come installed with anti-virus software typically Norton or McAfee anti-virus. If you do not have anti-virus software installed, purchase one and install it on your computer. Register your copy via the Internet. You will be able to update it with the latest signatures so that your version will up to date to deal with the latest viruses. I would highly recommend that you scan all your files on your computer as well. Typically, when scanning your system for viruses, anti-virus programs default to scanning only your boot and system files. Again, I highly recommend you select scanning **all** of your files. Viruses named "Trojan Horses" are viruses that disguise themselves as normal files only to come to life on a predetermined day/time to wreak havoc to your system, hard drive or individual files as was previously mentioned in the Distributed Denial of Service (DDoS) section.

Keep in mind any removal media that you use, borrow or bring home from the office. Make sure you set your anti-virus program to scan all files, not just program files, but **all** files during run, open, copy, move, create or downloading mode. This may slow your day-to-day computing speed down a little but your piece of mind will be much higher. And speaking of downloading, caution, caution, caution. In this day and time of mp3 music download craze and a thousand and one other download options to speed up your computer, speed up your modem's Internet connection, etc., make sure your anti-virus program scans everything. There are a lot of hackers that just setup files for you to download thinking you're getting a music or video file. Just simply use caution, caution, caution, scan, scan, scan…

Lastly I recommend that you set your anti-virus to perform a monthly update of software or twice a month if you're a little more couscous. These updates can be set to run automatically while you're not using your computer as well.

3. Updating Your System Files

Updating your system files is critical to ensuring that your operating system and application bugs (coding problems and vulnerabilities) are corrected. Microsoft is well known for shipping out their operating systems so that the consumers (you) find and report problems them back to Microsoft to repair. Fortunately, with the advent of the Internet, Microsoft will post repairs to specific problems on their web site that you can download typically for free. These operating system and application repairs are commonly referred to as "patches".

The key for the novice home user is keeping abreast of technical issues that may be confusing, complex and simply difficult to understand and know whether to download and incorporate into your system. Microsoft does an admirable job putting together a fairly intuitive web site for the novice and highly technical user. I recommend logging onto Microsoft's web site on a monthly basis and look at "Today's News" for up-to-date information on current issues. For instance, Windows XP and other Windows system users running Universal Plug & Play can find the patch for a security breach posted for download and repair. The download instructions are easy to follow and install. Other areas recommended to inspect on Microsoft's web site include the following.

- **Resources** – Probably the best area for novice users is the Resources page. Allows users to search, download, look at frequently asked questions (FAQs), post your own questions and look at other Microsoft user questions and answers, and contacting Microsoft online.

Search our Database of Support Articles
Search across the Knowledge Base for articles designed to answer your product questions.

Download Software
Find software updates, service packs and patches, device drivers, and complete Microsoft products.

Product Support Center - Important Information by Product
Common issues, instructions, latest versions, and related sites for your product (FAQs).

Post Questions in our Newsgroups
Browse by subject and collaborate with other people using Microsoft products.

Contact Microsoft Online
Send your question to our support professionals over the Internet. You will need to log in using your Passport account.

Problem areas that I find for most users performing downloads is the size of the patches. Most users are still connected via 56kbps dial-up and most patches require several minutes to download. If you're a broadband user most downloads only take a few minutes to complete.

If you're a home user that prefers to keep it as straight forward as possible then you should focus on maintaining up-to-date patches on your operating system and all Internet applications. Your Internet applications include but are not limited to Microsoft's Internet Explorer, Outlook, Outlook Express, Winamp (mp3 player) as well as other mp3 players, Netscape Navigator and Netscape Mail.

4. Backups

Another key aspect to protecting your system from virus corruption is to perform periodic backups of your computer system. Your system at a minimum comes with a floppy drive that can be used to backup critical files such as documents, spreadsheets, and home accounting files from Quicken or Microsoft Money. Hopefully your system comes with a Iomega Zip drive, Iomega Jaz drive, standard tape drive, or CD re-write drive, which will make performing backups much less painful because these media types can hold 50 to hundreds times more data than a standard floppy can.

Today it has become increasing more difficult to backup your entire system without a backup drive that can support large amounts of data. Given the fact that applications utilize large amounts of disk drive space the simplest way to maintain the integrity of your data is to backup your data only. Your data is absolutely critical to you and typically hard to replace. Your applications such as Microsoft Word, Excel, Quicken, Netscape, games, etc. can be reloaded from their original media such as CD or floppy and thus is not necessary to backup.

I recommend that you perform a periodic (monthly) backup of your important files. Any files that you deem to be extremely important I recommend you back them up more often or on an as needed basis. Take it from experience, as many of us now maintain our own personal banking on our computers, losing weeks or months of your checkbook entries can take several hours or days to recreate and reenter. Performing a simple backup to floppy or other media of these and other important files from a potential virus can be a lifesaver.

5. Encrypting Your Data

If you feel that the e-mails and data that you send to other people across the Internet is important enough that you would not want anyone easily viewing this information, then you should consider encrypting your data. One of the more popular encryption methods and easy to implement and utilize is a secured public/private key method call Pretty Good Privacy or PGP for short. In order to use PGP you will utilize both a public and private encryption key. That means that it uses two different keys for encrypting and decrypting data. This typically is somewhat confusing that most people have trouble with using it. Every user will have their own public and private key pairs. One is called a "private key", which is used with your password to decrypt all your encrypted messages and files. The other key is called your "public key", and this is given out to the friends and associates you wish to communicate with. They use your public key to encrypt a message sent to you and you will then use your private key to decrypt it. You also use your own public key

to encrypt your own files, and then use your private key to decrypt them.

The wonderful aspect about PGP is that giving out your public key does not compromise your security. In fact, you must give out your public key to anyone who wants to encrypt a message to you. It does not matter if a hacker gains access to your public key, because all they can do with it is encrypt messages that only you will be able to decrypt by using your private key. Once you install PGP you will be prompted to generate a pair of keys (public and private) and give out a copy of your public key to all your contacts. You will also be collecting the public keys of all your contacts as well and they will be stored on what is called your PGP key ring.

If you truly interested in implementing this level of data security go to the following web site. The International PGP Home Page at http://www.pgpi.org/doc/pgpintro/.

Conclusion

Emphasized over and over is the need for home users to perform a little due diligence in their spare time to provide their home computer a better level of protection from Internet attacks. Let me state that again. A "*better level* of protection from Internet attacks". There are no absolutes and total protection of any computer attached to the Internet. But what the home user can do is to protect themselves from almost all of the viruses and worms that present the biggest threat to home user computers. Perform the monthly updates of your anti-virus and firewall software, operating system, Internet browser, and e-mail viewer patches.

References:

CERT Coordination Center, Carnegie Mellon, General Info. - http://www.cert.org/nav/index_main.html

CERT Coordination Center, Carnegie Mellon, Home Network Security - http://www.cert.org/tech_tips/home_networks.html

Jolo with help from wmono, mendel, Dancr, GreyFoxx, wcoast, and many others!. “Denial of Service or "Nuke" Attacks”. 21 February 2001. URL: http://www.irchelp.org/irchelp/nuke/

Ludwig, Katherine. "Security Awareness: preventing a Lack in Security Consciousness." 25 May 2001. URL: http://www.sans.org/infosecFAQ/aware/lack.htm

Wilson, Zachary. "Hacking: The Basics." 4 April 2001. URL: http://www.sans.org/infosecFAQ/hackers/hack_basics.htm

Diamond, Bruce. “Why Small Businesses Need to Secure Their Computers (and How to Do it!)”. 16 August 2001. URL: http://rr.sans.org/securitybasics/need_sec.php

Vnunet.com. “MP3 users warned about security threat”. 01 December 2000. URL: http://www.vnunet.com/News/105278

Steve Gibson Research. “Personal Firewall Scoreboard” Current. URL: http://grc.com/lt/scoreboard.htm

Trigaux, Robert. St. Petersburg Times Staff Writer. “The underbelly of cyberspace” 14 June 1998. URL: http://www.sptimes.com/Hackers/underbelly_of_cyberspace.html

Edward W. Felten, Dirk Balfanz, Drew Dean, and Dan S. Wallach. Princeton University. “Web Spoofing: An Internet Con Game”. Revised February 1997. URL: http://www.cs.princeton.edu/sip/pub/spoofing.html

Philip Zimmermann, "PGP User’s Guide, Volume 1", ftp://ftp.pgpi.org/pub/pgp/2.x/doc/pgpdoc1.txt

The International PGP Home Page. “How PGP Works” Current. URL: http://www.pgpi.org/doc/pgpintro/