# Global Information Assurance Certification Paper

# Broadband Security Concerns For Home and Remote Users

Ver. 1.3

Jaeson Rebeyro

January 29, 2002

**Summary**

This paper is written for users who are considering getting broadband for their home or remote office, it deals with the different varieties of broadband and their pros and cons. It also informs users of the security concerns of having broadband and how to protect themselves from intruders**.**

Because the use of broadband allows the user to keep their ports open for an unlimited amount of time, this can become a danger, not only for intruders damaging the users personal information, but for hackers who use open ports to launch attacks. Some of the aspects that will make the use of broadband a secure environment are the use of antivirus programs, firewalls, backups, and keeping the applications and operating systems updated.

**Introduction**

With the growing need for information, the use of the internet has increased, more people are using the internet to check on weather, sport scores, breaking news, video clips, music, shopping and most of all doing research on anything that passes through their mind.

Many companies see this trend and provide more sophisticated web sites that require faster speed. As a result, home users with dial-up access to the Internet find accessing these new sites slow. Since dial-up can only provide up to 56kbps of bandwidth, this makes it obsolete.

Broadband is a technology that delivers high speed Internet connection to your home or office and is always connected to the Internet. Everyone wants to be your Internet provider, the two most common mediums for delivering broadband is cable and DSL. These two mediums can deliver bandwidth from 128k to 8Mbps.

There are many other mediums like satellite, wireless, frame relay and ISDN. We will focus on cable and DSL because they are widely used to provide broadband to home users. Then the latter part of this paper we will dive more into why you need to secure your connection and how to do it.

**Cable Modem**

Internet access is delivered to homes via broadband coaxial cables originally designed to deliver broadcast television signals. A home user may experience speed from 500kbps to 1.5 Mbps depending on the network design and load.

Most cable systems use a share access design, much like an office LAN. Because they are shared, bandwidth decreases as the number of subscribers increases (See Fig.1). 200 subscribers sharing a 27 Mbps will get about 137kbs throughput.

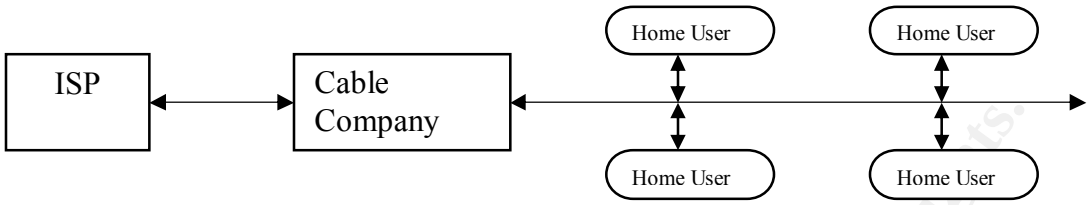


Figure 1: Topology of Cable Internet access
Figure created by Jaeson Rebeyro

**DSL**

DSL stands for Digital Subscriber Line, it's a broadband technology that uses telephone lines and digital coding to create a connection from your home to the Internet.
There are different flavors of DSL available today, the two most common ones are ADSL (Asymmetrical Digital Subscriber Line) and SDSL (Symmetrical Digital Subscriber Line).

ADSL, is designed for the residential consumer market An ADSL connection transmits data at faster speed downstream, from the internet to a home user, than upstream, from your pc to the internet. This type of connection can support speeds up to 8Mbps downstream and 1Mbps upstream.

SDSL transmits data at the same speed in both directions, it is mainly used by commercial clients. It can support speeds in both directions up to 2Mbps.

DSL is not available everywhere due to the technology limits. Because DSL frequency travels through copper, the frequency erodes after it travels a distance more than 12,000 feet. That's why DSL is only available to subscribers that are about 12,000 feet from the central office.

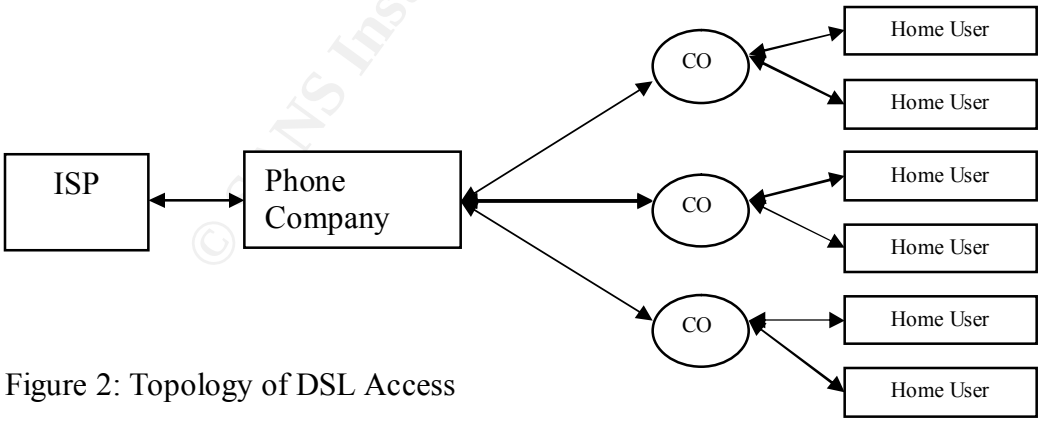


Figure 2: Topology of DSL Access

Figure created by Jaeson Rebeyro

**Down side of Broadband**

To the user convenience, both of these broadband technologies do not require you to dial the internet provider when you need to be on the internet, once connected your connection to the internet is always on, unless you turn off the cable or DSL modem, as a result these type of connection looks very attractive to hackers because most home users are not aware of the latest exploits and do not patch up their systems and have them wide open.

**Do I need to be concerned?**

The computers at home are use to do banking, investing, shopping research, chatting and sending email to friends and family. All this information is stored on your computers and you may not want intruders snooping into your personal business or using your information against you. These intruders can also send bogus email on your behalf, monitor your moves and even destroy your systems.

Furthermore it is important to prevent intruders who don't care about your personal information but use your computer and Internet connection to launch attack to other systems like government agencies or financial institutions.

**How do they get into my system?**

The Internet is constantly being scanned for open ports on the internet, users with broadband make easy targets because most of their connection is unsecured. Port scan is a practice used by hackers to scan an IP address to find out what services like web server, FTP server, windows sharing, Nabster, Mophouios or others, your pc is running. An IP address has 131,070 available ports. Every application and service that communicates via TCP/IP uses ports.

Below is a list of common ports you may find on a PC connected to the Internet

| Services | PORT | Comments |
|---|---|---|
| HTTP (web) | 80 | If you are running a web server or personal web server |
| FTP | 21 | File sharing, this is included in MS Internet Information Server |
| NetBios Datagram | 138 | It is primarily used by the SMB browser service that fills in the information within the "Network Neighborhood" icon |
| NetBIOS name service | 137 | This is how NetBIOS-based services find each other on a NetBIOS network |
| Net Meeting | 389,522,626,1503,1720,1731 | Microsoft's NetMeeting is video-conferencing style software. |

For more information on TCP ports see http://www.camden411.com/tcpipfaq/ports.html

After a hacker finds out what operating system and services are running, they then try to exploit their weakness to get full access to the system. Now that the hacker has access to you system, they may put Trojan commonly known as backdoor programs, these programs give the hacker full remote access to your system.

A hacker may also use your compromised pc to attack another system like a government agency, and all fingers will be pointed to you.

Another form of invasion to your pc or home network is through worms and viruses, these infections mainly spread through email, file sharing, web browsing, email attachment etc. There are over 53,000 viruses out on the Internet today, and that number is growing. They can render your PC and data useless and even send data out on the Internet and attack outer users.

**Now I am scared, what do I do to protect my system?**

There are several steps you can take to protect your system, they don't substitute each other but are complementary. The following procedures will give you a better understanding of the different security precautions available.

**Use Strong Password:**
The majority of computer breaking can be traced back to poorly chosen passwords, some times it is the only obstacle that protects your computer from the hacker.
If an intruder can guess or hack a user password, then the intruder will be able to operate your PC with no restriction, and if this intruder uses your pc to do damage, you will be blamed.

A good password is a private, secret, easy to remember and not guessable. Below are a few guidelines to follow while creating and maintaining a password.

- It is a good practice to change your password on a regular bases
- Keep it between 6 and 8 characters long (longer the better)
- A mixture of upper and lower case letters, having numeric characters
- Create a password that you can type quickly
- Never create a password with a word that is found in dictionary
- Never recycle your password
- Never write down you password.
- Do not use your name, spouse's, partner's, pets, or child's name
- Do not use you social security or license plate number.
- Do not use anyone's birth or anniversary date.

Below are a few examples of bad passwords that are easy to crack with programs that are available for free over the Internet.

Abc123
Two4two
Love2sing
Jason2work

A method that will help you create a strong password is changing sentence into password. This is one of the easiest to remember but hard to crack method. First find a phrase familiar to you and that you will always remember, then create the password using the first character of each word of the phrase, for example:

Phrase: I like to read books at home
Password: 1l2rb@h

Phrase: My birthday is on October 13th.
Password: Mbi0O13th

Phrase: My daughter's name is Andrea and she is 9
Password: MdniAasi9

Following the example you can create passwords that will be easy for you to figure out at any moment, but it will take a long time for a brute force password cracker to find. This does not mean it cannot be broken, all passwords can be broken and that is why the follow up to this procedure is to change your passwords on a regular bases.

**Use Virus Protection:**
A computer virus is a self-replication program containing programming code that copies itself and can infect other programs by altering or changing their environment. The term Virus is used frequently to also classify other forms of programs that infect your system like Worm and Trojan horse.

A Virus can corrupt files, reformat disks and even make your pc unusable; the better one tries to spread them.

A computer worm is a self-containing program that is able to spread functional copies of itself or its segments to other computers, mainly via a network. Unlike viruses, worms do not need to attach themselves to a host program.

A Trojan horse is a program that disguises itself as a different program or hides behind a program.

To protect yourself from viruses you should make sure you have an anti-virus program installed on your computer such as Symantec Anti-Virus, or McAfee Virus Scan.

In most cases you can protect yourself from viruses with the observation of some simple precautions. Below is a list of precautions you can take to prevent your pc from getting infected.

- Never accept files (via email attachment, file transfer etc.) from people you do not know. The most common way to get a computer virus is through an e-mail attachment.
- Scan floppies before using them because they could be infected with a virus.
- Do not boot from a floppy.
- Do not download programs from the web unless it is a reliable source and make sure your virus program has been updated first.
- It is good practice when using the internet to verify that the person sending you a file is indeed the person you think it is by asking them to provide information known only to the both of you.
- Pay attention to files that are disguised ("Mypic.jpg.exe"). You will usually only see the final extension (eg. "exe") after you have saved the file to your hard drive. Files that are disguised usually contain malicious code and should be checked with updated anti-virus software.
- Use an updated anti-virus program to scan all of the files you download.

**Install Firewall/Router**

A router is a device that joins two or more networks together enabling the networks to communicate between them (See Fig.3). Most DSL and Cable internet provides a device (router or modem) for your home network or PC to communicate to the internet. What this does is leave your connection open for intruders to cause damage.

To solve this problem a firewall needs to be installed between the providers' router/ modem and your home network or PC.

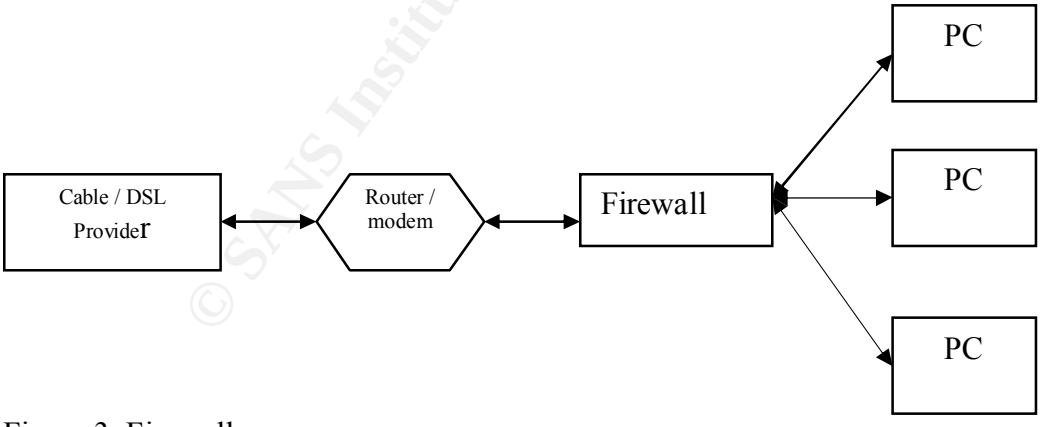


Figure 3: Firewall
Figure created by Jaeson Rebeyro

A firewall is a barrier to keep unwanted intruders from looking or entering your network or PC, it is a device that filters incoming traffic, every packet is screened and checked against the rules or filters preset by you. For example you can configure the firewall to let all traffic leaving your

network or PC through the firewall and block everything that is trying to enter your system. By doing this, if an intruder tries to scan you network with a port scanner to find out what ports you have open, they will not be able to see anything unless you have opened ports on the firewall.

There are many manufactures that combine the router and firewall together and design the configuration of these devices easy to use so that the novice users can configure them. These routers/firewalls are also known as DSL/Cable routers and are priced between $90 and $300.

One of the biggest advantages of using them is that you can share your DSL/Cable internet connection with more than one PC. Manufacturers like Linksys, Siemens, Netgear, SMC and many other companies make this device.

**Use Personal Firewall**
A personal firewall is a powerful security software package that acts as a door for your computer's incoming and outgoing connections. Based on your configuration, a firewall will only allow authorized communications to pass. Most of the firewalls are self-configuring which enables all traffic from your workstation to get out and blocks everything coming in, unless you approve it.

A firewall keeps a log of all attacks that have attempted to get into your system, you need to check this log on a frequent basis to make sure your configuration is working effectively.

ZoneAlarm, Tiny Personal Firewall and Sygate Personal Firewall are available free for personal use, there is a fee if you use it for business.

**Turn off File Sharing**
On most Microsoft systems this feature is on by default and it enables you to share files over your local network. If you do not need this feature, disable it.

However, if you have to use it make sure you password protect your share by using strong password.

To disable file sharing on Windows 95, 98 and ME follow the steps below:

- Double click on *My Computer* icon. My computer window will open.
- Double click on *Control Panel*, this will open a new window.
- Double click on Network, this will open a Network window.
- Left click on *File and Print Sharing*, the File and Print sharing property box will appear with two options, Uncheck both boxes and click *OK*.
- Double click on the TCP/IP protocol that is bound to your network card, this will bring up the TCP/IP property window, select the *Binding* tab
- Clear the box beside *File and Printer sharing for Microsoft Networks* and Click Ok.
- You will be back to Network Properties, click *OK* again.
- You will be prompted to restart your system, click *OK*.
- Your system will reboot.

To disable file sharing on Windows NT follow the procedure below:

- Right click on *Start* > *Settings* and then *Control Panel*
- Double click on *Services*, this will bring up the Services window.
- Scroll to *Server Services* and click on *Stop.*
- Click on *Startup* and set it to *Disable*
- Click *OK* and click *Close*

By default in Windows 2000 Professional file and print sharing are enable, to disable them, follow the steps below.

- Right click on *My Network Place,* left click on *Properties*, this will open *Network and Dial-up Connection* properties
- Right click on *Local Area Connection* and click on *Properties,* this will open *Local Area Connection* properties.
- Scroll to *File and Printer Sharing for Microsoft Networks* and uncheck the box beside it.

I recommend restarting your system and this will disable file and print sharing.

If you want to turn off file sharing on MAC, the following link has good instructions
http://site.lisco.com/support/wireless/mac/macfileshare.html

**Keep your operating system and software up-to-date**
One of the many ways an intruder gets into your system is by first finding out what you have running on your system. Once they accomplish that, they look for security holes in the application you have running. Practically every operating system and application manufacturer distributes patches and updates on a regular basis, these patches and updates need to be applied to your system as soon as they are available. Make it a good habit to check the manufacture site for these updates.

Some of the famous attacks like the CODE RED and the NIMDA worms used well-known Microsoft security holes to compromise the system. CODE RED worm infected hundreds of thousand of computers and made them zombies to attack one of the servers that hosted the White House web site by flooding the site with bad requests. The NIMDA worm spread via emails, network share, web server to client and by back doors left by CODE RED and SANDMIND worm.

Patches for this security hole were available a month prior to the attack and if the patches would have been applied, the infection would not have been so great.

Microsoft has embedded a Window updated on its newer operation systems, Windows 98, ME, 2000, and XP. This tool makes it easy and painless to keep your system up-to-date. Once you are connected to the site, the Windows updater scans your system to see what you have installed and gives you a list of components you need to install to keep your system up-to-date. Some of the updates are categorized as Critical Update, which fix known problems.

To get to this updater tool, click on Start>Windows Update and follow the on screen instructions. Make it a good habit to check it once a week. In the past I used to be afraid to do this because of the bad reputation Microsoft had regarding updates crashing PCs, but Microsoft has improved and now I feel comfortable applying all their security patches they put out.

**Backup your systems**
This is one process that is least done and one of the most important ones, the value of backing up your data is realized when your PC crashes or when an intruder destroys your systems.

In the 80's and 90's you could backup data on floppies, with technology improving, hard drive size on PC have increased from 500 Megs to 40 GB. This causes problems for home users to back up their system or data.

Fortunately technology on storage media has improved too, new devices like CD-RW, Zip, Jazz drives are available with new PC or available for upgrade, these devices can hold from 250 meg to 600 meg and they range between $ 100 to $ 500. The media ranges between $1 and $100 depending on the type of media you use.

There are other backup solutions like tape backup that do a faster job and can hold a large amount of data, but they range between $300 and $1500.

Now you have the device you also need software to manage it, luckily most operating systems come with backup software, although you can purchase third party software that does a better job.

Run your backup schedule based on how often you make changes to your file or system settings. Be familiar with the restore process, do a dry run and make sure you know how to recover data.

Another option is to access companies like NetMass,VirtualBackup and Connected now offer online backups, they use your high speed connection to upload data from your PC to a centralize storage which you can access at any time, it is a good way to keep data offsite just in case there is a natural disaster. If you use this system it is recommended to backup only important file.

**Subscribe to a security list server**.
This is a good way to keep your self up to date with technology and also to keep ahead of the game when it comes to network and pc security. Many security conscious organizations like sans.org, cert.org and incidents.org have websites that publish up to date information and can send you an email when something new comes up.

**Conclusion**

Getting broadband is relatively easy, but keeping intruders from taking advantage of your broadband connection to harm your system and other systems is of concern. Following all the guidelines stated in this document should keep your pc free from attack.

At first it may all seem very overwhelming but that is nature of the beast. We lock the door in our homes and cars, but that is still not enough, so we install alarms and other devices to protect our self. The same thing applies to computer security.

**List of References:**


Broadband FAQ
http://www.broadbandcompass.com/search/jsp/learnmore/index.jsp?partnerID=bbl

Kim Thomas "Building a Secure Home Network" July 26, 2001
http://rr.sans.org/homeoffice/home_net2.php

Jeff Tyson "How Firewalls Work"
http://www.howstuffworks.com/firewall.html

Earl Charnick "Getting the most security out of the Linksys cable/DSL router" November 30, 2001
http://rr.sans.org/homeoffice/linksys.php

Hanz Makmur "Securing and sharing your home broadband connection"
http://please.rutgers.edu/show/firewall

Faq on Virus-L/comp.virus
http://www.faqs.org/faqs/computer-virus/faq

CERN Security handbook
http://consult.cern.ch/writeup/security/security_3.html

Bruce Schneier "Secrets & Lies"
Wiley Computer Publishing ISBN 0-471-25311-1

Randall Nichols, Daniel Ryan and Julie Ryan "Defending your Digital Assets"
RAS press ISBN 0-07-213024-5