Global Information Assurance Certification Paper

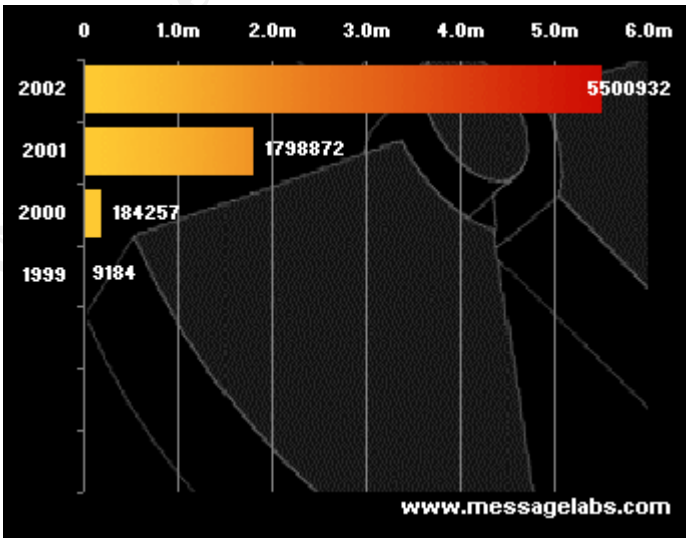
Security & Privacy at Home

GSEC 1.4, Option 1

Brian Porter

The vast majority of home computer users are not information security experts. Many do not have the knowledge, experience or resources to effectively protect their systems and data from compromise. You do not however, need to think in binary to be able to establish a basic foundation for protecting a home system. The information that follows provides the building blocks for securing your home computer from hackers, viruses and the curious eyes of others. These principles can be applied to various operating systems (Windows®, Macintosh®, etc.) and many times will apply to computers in a small business environment as well. After reading this paper you'll have a better understanding of the importance of information security in general and will be able to apply it to your home computer environment.

Why should I care? Good question. You may not think that your home computer is at risk of being compromised. To better understand let's look at the actual definition of risk. Risk is generally defined as vulnerability x's threat. Is your home computer vulnerable? Yes – especially if you are not correctly using anti-virus and firewall applications on your Internet connected computer. We'll discuss these essential tools in more detail in a moment. OK, so maybe your computer is vulnerable, but what's the threat? After all, our formula is risk = vulnerability x threat. Zero threat multiplied by any vulnerability would be zero risk. "No one would want to hack into my computer, we just use it for games and surfing the web." You may be correct – your computer could be extremely uninteresting from a sensitive data perspective. Unfortunately most viruses, trojans, worms and the like spread without discrimination. The diagram below depicts the staggering increase in the number of viruses each year. "Klez", one of the most active viruses in 2002, has been intercepted over 2.8 million times in 205 different countries by the SkyScan service between April and September of 2002[1].



Number of viruses intercepted by MessageLabs' SkyScan service since 1999.
The 2002 figures represent year-to-date figures as of this writing (9/2002.)
http://www.messagelabs.com/VirusEye/default.asp?by=all

[1] MessageLabs. "VirusEye". http://www.messagelabs.com/VirusEye/default.asp?by=all (14 Sep. 2002)

In addition to destructive viruses, your computer could provide an excellent host for a distributed denial of service (DDoS) attack. In this scenario your computer is one of many computers being infected with a malicious program that could be used to flood another network, website, etc. with data, causing the attacked network to be unable to respond to legitimate requests.

Hopefully by now you're starting to get the picture. Any computer, especially one connected to a network or the Internet, is a potential target. This is the threat in our equation. Reducing the threat is difficult in this age of the information superhighway. We've become accustomed to having instant access to information and this requires connectivity to other computers. Since it's unrealistic to think you can unplug your computer and disconnect it from the rest of the world, let's look at some ways to reduce the vulnerability.

Anti-virus Software

Earlier we said that the lack of, or incorrect use of, anti-virus and firewall applications could greatly increase the vulnerability of your computer. Let's start with viruses, trojans and worms. What is a virus? According to Trend Micro™ a virus is a program that has the ability to replicate, or make copies of itself, and spread to other files[2]. Many of these viruses carry destructive payloads and will attempt to damage the computer by altering or removing critical files. In the beginning viruses we're usually transmitted via floppy disks. Now viruses can be transmitted much more quickly via e-mail or via files available for download on the Internet. Worms and trojans also pose a significant threat to unprotected or poorly protected systems.

Terms (definitions by Trend Micro™)[3]
Virus: a program that has the ability to replicate, or make copies of itself, and spread to other files.
Worm: Worms are viruses that replicate and propagate to other systems. Typically, they send exact copies of themselves over the network either via email, through network shares, or sometimes over security holes or exploits. However, there have been a few noted worms that can both infect files and replicate over the network.
Trojan: A Trojan is malware that performs unexpected or unauthorized, often malicious, actions. The main difference between a Trojan and a virus is the inability to replicate. Trojans cause damage, unexpected system behavior, and compromise the security of systems, but do not replicate. If it replicates, then it should be classified as a virus.

[2] Trend Micro. "Glossary of Virus Terms"
http://www.trendmicro.com/en/security/general/glossary/overview.htm
[3] Trend Micro. "Glossary of Virus Terms"
http://www.trendmicro.com/en/security/general/glossary/overview.htm

Now that we understand what viruses, worms and trojans are – how do we protect our computers from them? The answer of course is anti-virus software. Anti-virus software is available from many vendors and comes in various forms. See the table below for some of the major players in the anti-virus market. Most anti-virus vendors make their software available for purchase and download directly from their website. In addition (as of the time of this writing) Trend Micro™ offers a free online virus scanning service, which can be accessed via http://housecall.trendmicro.com/ .

Where to obtain anti-virus software:

Company & Product	Website
Symantec™ (Norton Antivirus™)	http://www.symantec.com
Network Associates (McAfee VirusScan)	http://www.mcafee.com
Trend Micro™ (PC-cillin)	http://www.trendmicro.com

Now you know why you need anti-virus software and you know how to obtain it. What's left? You now need to understand a few basics on using the software. The first and most important rule is to ensure your anti-virus software is always running. Normally on a Windows PC the software will display an icon in the "systray" near the clock in the lower right-hand portion of your screen. Double-clicking the icon should open the program and allow you to view and change settings. One of the most important settings to have enabled is an automatic update service. This option tells the software to automatically connect to the vendor's server to check for updates. Updates are usually for the definition files, which is what the software uses to detect viruses. New viruses are being constantly developed, the older your definition files are, the more vulnerable your system is. In addition to frequent updates you should also create a recovery disk and update it frequently. The recovery disk can provide the support you need when a virus prevents your computer from booting. Without a recovery disk you may need to re-install the operating system or in a worst case scenario reformat the hard drive and lose all data.

The table below recaps the most important points related to anti-virus software.

Points to remember:

What	Why
You must have anti-virus software installed on your computer.	The exchange of data between computers makes them vulnerable to viruses, worms and trojans.
Your anti-virus software must be running at all times.	Viruses can react as soon as the computer begins to boot.
Your anti-virus software must be configured to check for updates regularly.	New viruses are created often; your anti-virus software needs to be updated just as often.
You should always have an updated emergency recovery disk available.	Many viruses will prevent your computer from booting. A recovery disk can save you from loosing all of your data.

Firewalls

Now that we have our anti-virus software installed and configured to automatically update, we can relax – right? Not yet. We've locked away the family's valuables, now we have to lock the doors. For that we'll need a firewall. Firewalls are used to restrict access to a computer or network of computers. The term comes from the thick protective walls installed in buildings, which prevent fire from crossing from one room or apartment to another. For our purposes we'll be looking at personal firewalls, which you can install on your home computer to provide a first layer of protection. Think of your personal firewall as a sort of filter. It allows you to specify how much or how little access you wish to provide to your computer, from the network it's attached to. Typically this means blocking unwanted Internet traffic from sources such as hackers, trojans, worms, etc. When a request is made to your computer the firewall intercepts the request and then based on the rules or settings you have configured, decides what to do with the request. Basic actions your firewall can take are to allow the request through or to block the request, preventing it from reaching its destination.

Ports? The destination on your computer is normally a port (think of this as a connection point, your computer has many ports) and that port may have an associated application listening on it. Here's an analogy that may help understand ports. Let's think of your computer as an apartment building and the applications on it as individual apartments. Your computer on a network, like the Internet, has an address. This is known as the I.P. address of your computer and no other computer on the network should have the same address. To access a specific application on your computer, another computer usually needs to specify the address (I.P. address) and the port. So for our analogy your computer's I.P. address is like the apartment building's street address and the port is similar to an apartment number, basically providing more specific address information. OK, why do you need to know what a port is? When attempting to connect to another computer, that computer must accept the connection on the port specified. When you connect to a web server it is generally allowing you to connect to port 80. This happens behind the scenes because your web browser assumes you want to connect to port 80 since that is the standard web port. Not convinced? Try this – Within your web browser navigate to http://www.google.com and then navigate to a command prompt. Using Windows this can be done by clicking "Start", "Run" and typing either "command" or "cmd". Once you're at the command prompt type "netstat" and press enter. Assuming you still have an active connection to Google (reload the page and try the netstat command again if needed) you should see something similar to the output below:

```
C:\>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    computer-name:1088     www.google.com:80      ESTABLISHED
```

What this is telling us is that we have an "established" connection to Google on port 80, using our local port of 1088. For our purposes we're mainly concerned with the port of the computer that's receiving the connection. Try connecting to Google on another port (http://www.google.com:81 for example) and repeat our netstat command – you'll see Google will not accept the connection, the browser will return an error and the nestat command will show a "syn_sent" status which basically means we sent the request to connect but haven't received a response from Google's server.

That is a lot of information on ports, but understanding the previous information will go a long way in understanding how to configure your firewall software. It will also help you understand why you may occasionally have a problem with an application on your computer that uses the Internet. What we want to do is what we saw in our Google example – allow legitimate access to our home computer but ignore or deny everything else. Most applications do not require you to allow inbound connections to your computer. Browsing the web and sending e-mail normally require you to initiate connections to other computers (servers) but rarely require those servers to initiate connections to you. Let's look at a few applications that may require your computer to act like a server and allow inbound connections. The most common categories are instant messaging applications, chat and video conferencing applications and internet gaming.

Application	Direction	Protocol	Port(s)
AIM (AOL Instant Messenger)	Inbound	TCP	5190
AIM (AOL Instant Messenger)	Outbound	TCP	4099
MSN Messenger - Messaging Functionality	Outbound	TCP	1863
MSN Messenger - Voice Functionality	Outbound	TCP	6901
MSN Messenger - Voice Functionality	Both	UDP	6901
MSN Messenger	Both	TCP	6891-6900
Yahoo Messenger	Inbound	TCP	5050, 80, *

* Yahoo Messenger will search for an open port if 5050 or 80 are not available on your computer for inbound connections.

Note: For more information on ports used by various applications consult The Internet Ports Database at http://www.portsdb.org. From this site you can search by application name (i.e. AIM) and have results returned on the related ports.

If you are using one of the applications above or a similar type of application, you may need to allow access to the required ports on your computer. This change will need to be made within the firewall software. If you do not already have a personal firewall installed on your computer you can consult the table below for some of the more popular versions. All three vendors below allow you to purchase and download their firewall products online. In addition, many newer operating systems include built-in firewalls. This is true for Windows® XP, Macintosh® OS X and most Linux distributions.

Company & Product	Platform	Website
Zone Labs (ZoneAlarm©*)	Windows	http://www.zonelabs.com
Symantec™ (Norton™ Personal Firewall)	Windows and Macintosh	http://www.symantec.com
Network Associates (McAfee VirusScan)	Windows	http://www.mcafee.com
Internet Security Systems™ (BlackICE™)	Windows	http://blackice.iss.net

*The Zone Alarm basic product is free for personal use.

After downloading and installing your firewall software you should have at least a default configuration that should provide basic protection. Take some time to read the manual or visit your vendor's website to ensure you're familiar the features of the application. You don't need to be an expert firewall administrator, but you should be aware of what the software is doing. Some of the personal firewalls, for example, can block the pop-up ads you see when visiting many websites. This can be handy but can also cause trouble if it misinterprets valid pop-up windows from sites such as your bank or broker as an ad. The general rule for configuring a firewall is to deny everything that you do not explicitly need. In other words, restrict as much access as possible and then make changes as needed in order to be able to function. This is why we discussed ports earlier – so when you load that new video conferencing application but can't get it to work quite right, you can verify you have your firewall configured to allow connections to the required ports on your computer. Use the Internet Ports Database we discussed previously to find out what application may be using a port you see referenced in your firewall's log file. If you see your firewall is repeatedly denying connection requests to port 1214, search the database and find out what the port is generally used by. It may be that new Kazaa file sharing application you installed which hasn't been working. Try opening the port and see if the application is now functioning. Remember - it's safest to deny all and then add access as needed.

Other Topics of Interest to Securing your Home Computer

E-Mail

The nature of e-mail makes it an easy conduit for malicious activity. Some of the most widespread and damaging worms have multiplied throughout the Internet via e-mail programs such as Microsoft® Outlook. Common sense and updated virus software will go a long way in protecting your computer from such attacks. Use common sense when opening e-mail from unknown sources and especially when opening attachments within e-mail, even if from a known source. Many worms are sent from one person to the contacts listed in their address book, thus giving the impression the e-mail is from a trusted source. If you're not sure contact the sender and ask them about the e-mail. The updated virus software comes into play when the common sense fails. Keep in mind however that newly released viruses, worms and Trojans can be in the wild for hours, if

not days, before updates are available for your anti-virus software. Again, common sense is essential.

Cookies

Many times unencrypted cookies are set by web sites which you visit which can leave potentially sensitive data unprotected on your computer. Examples could be login information for a particular web site or information you submit via a website's form such as your name and address. Many sites, which take security seriously, will encrypt the data they save within cookies on your computer. This prevents someone who can access the data on your computer from being able to easily read through the data stored in the cookies. There are many misconceptions about cookies. Cookies are not viruses and they do not read all of the information on your hard drive. Cookies are most often used to store information (such as your zip code on a weather site) and maintain or track state. Here's a simple example of what we mean by maintaining state – the HTTP protocol used on the web was designed to consider every request individually. So when you navigate to a web site and load page one, that is one request. When you load the second page, that is a second request. The problem is the server can't easily tell that you made both requests in sequence. This is obviously a problem if you are on a site completing an application on multiple pages, as the server would not know to append the results of the second page to the first and consider them one. An simple way around this is to use cookies. The server can set a cookie saying you are user one when you load the first page. When you load the second page the server checks for the cookie so it knows what user you are – one. This way the server can maintain the state throughout the transaction. Most concerns regarding cookies come from their usage to track visits to web sites. An excellent explanation of this concern provided by the World Wide Web Consortium is below.

> *When a user first connects to the DoubleClick server to retrieve a graphic, the server assigns the browser a cookie that contains a unique identification number. From that time forward whenever the user connects to* any *Web site that subscribes to the DoubleClick Network, her browser returns the identification number to DoubleClick's server, allowing the server to recognize her. Over a period of time DoubleClick compiles a list of which member sites the user has visited and revisited, using this information to create a profile of the user's tastes and interests. With this profile in hand the DoubleClick server can select advertising that is likely to be of interest to the user. It can also use this information to compile valuable feedback for its member Web sites, such as providing them with audience profiles and rating the effectiveness of the advertisements*[4].

There are many ways to manage what cookies are being set by the sites you visit. One of the simplest is to use one of the newer web browsers which provide tools to manage and view cookies. Three of the most popular are below.

[4] Stein, Lincoln D. "WWW Security FAQ: Client Side Security". Version 1.6. 28 July 2001. http://www.w3.org/Security/Faq/wwwsf2.html#CLT-Q10 (12 Oct. 2002).

Browser	Where to Download
Netscape	http://www.netscape.com/download
Microsoft Internet Explorer	http://www.microsoft.com/ie
Opera	http://www.opera.com/download/

You can set any of the browsers above to prompt you prior to allowing a cookie to be stored on your hard drive. In the prompt, the name of the server should be listed. Check the name and if it does not appear to be familiar (name of your bank, e-mail provider, etc.) you can block the cookie. This method is suggested over blocking all cookies as many web sites will not function properly if your web browser will not accept cookies.

Peer to Peer (P2P) or File Sharing Applications

Peer to peer applications gained fame with Napster some years ago and have continued to grow in popularity ever since. These applications allow for millions of Internet users across the globe to easily share data and files with each other. There are of course security and privacy concerns with these applications. From a security perspective most of these applications require that you allow others to connect directly to your PC. Ideally these connections are limited to the purpose of allowing the P2P application to exchange files, however it opens the possibility of an attacker exploiting the connection to gain unauthorized access to your computer. There is also the possibility that sensitive information can be inadvertently shared due to misuse of the application. This misuse most commonly comes in the form of unintentionally sharing files. Most P2P applications are used to share collections of music (MP3) and video files, as well as programs. When an inexperienced P2P application user mis-configures their software they can share many additional files – and in a worse case scenario the entire contents of the machine. These files can include cookies (which we discussed earlier), financial information files (Quicken, Microsoft Money, etc.), e-mail, password files and more. Finding these files for an attacker is as easy as typing the default filename (i.e. qdata.qdf for Quicken) into a P2P application and pressing search. The P2P application will then scour millions of online P2P users for the requested information. This is made easier due to the fact that many P2P applications share a common network (Gnutella is one of the most common).

If you plan on or are currently using a P2P application you need to:

(a) Have *current* anti-virus software installed and running.
(b) Have personal firewall software running and properly configured.
(c) Ensure you are not unintentionally sharing any files.

Most P2P applications allow you to view the files that you are currently sharing. In addition to potentially divulging private information, P2P applications also increase your computer's vulnerability. Most P2P applications act as servers and therefore require your computer to have open ports which other P2P

users can connect to. Risks of P2P include the transmission of viruses, worms and Trojans which we discussed earlier. More recently worms have been released which specifically target P2P applications. Usually these worms are disguised as frequently requested files in order to increase their likelihood of being downloaded.

Is Your Computer Acting Strange?

The first question I usually ask when a friend or family member queries me regarding a problem with their computer is, "is your anti-virus software current?" In many instances a computer running abnormally slow or failing to boot can be attributed to a virus. If this is the case ensure your anti-virus software is running and verify it has been updated recently. Some viruses will prevent your anti-virus software from running, but will still load the icon to give the appearance everything is fine.

Passwords

A great deal of compromises involve passwords being guessed. Most likely, even on your home computer, you are required to use passwords. Your Internet Service Provider, web-based e-mail and many other services require you to enter a password in order to prove you are an authorized user of the system. This password can be the key to your computer, e-mail messages or sensitive documents. Hackers understand that many people use weak passwords and also understand that guessing a weak password is much easier than having to break into a system via another route. Why disable the alarm system and crawl through a window if you can find a key to the front door? For these reasons having a strong password is a must. The CERT®/CC defines the characteristics below for a strong password[5].

Eight or more characters
Upper and lower case letters
Punctuation or other special characters
Not written down (easy to remember)
Can be typed quickly (prevents "shoulder surfing")

A useful tool in understanding the differences in strength among various passwords can be found at the Security Stats web site (http://www.securitystats.com/tools/password.asp). This tool will test a password you've entered and even provide specific feedback on what you can do to make the password stronger. Remember - don't give away the key to the front door.

Any computer, especially one connected to the Internet, is at risk of being compromised. The lack of anti-virus or firewall software, mis-configured applications and weak passwords are just a few of the factors that increase our vulnerability. The threat is increased as we connect to the Internet, and even more so when we use applications such as peer-to-peer file sharing or instant

[5]Howard, Dr. John D. "Policy Implications and Recommendations". http://www.cert.org/research/JHThesis/Chapter14.html (12 Oct. 2002)

messaging, which allows others to connect directly to use. We may never be able to eliminate the risk completely, but by using common sense and the practices provided in this guide, we can certainly reduce it significantly.

References

MessageLabs "viruseye, virus count"
http://www.messagelabs.com/VirusEye/default.asp?by=all (14 Sep. 2002)

TrendMicro "Virus Primer"
http://www.trendmicro.com/en/security/general/virus/overview.htm (14 Sep. 2002)

Good, Nathaniel S., Krekelberg, Aaron. "Usability and privacy: a study of Kazaa P2P file-sharing".
http://www.hpl.hp.com/shl/papers/kazaa/KazaaUsability.pdf (12 Oct. 2002)

Stein, Lincoln D. "WWW Security FAQ: Client Side Security". Version 1.6. 28 July 2001.
http://www.w3.org/Security/Faq/wwwsf2.html#CLT-Q10 (12 Oct. 2002).

Carnegie Mellon University CERT Coordination Center. "Home Network Security". 5 Dec. 2001.
http://www.cert.org/tech_tips/home_networks.html (3 Nov. 2002).

Security Stats.Com, Inc. "Password Strength Meter" 2000
http://www.securitystats.com/tools/password.asp (3 Nov. 2002)

The Internet Ports Database. "PortsDB". 17 Jan. 2002.
http://www.portsdb.org/ (3 Nov. 2002)

Whalen, David. "The Unofficial Cookie FAQ". Version 2.6. 8 Jun. 2002.
http://www.cookiecentral.com/faq (3 Nov. 2002)

America Online. "AIM | FAQ | Connection"
http://www.aol.com/aim/faq/connection.html#noLan (3 Nov. 2002)

Microsoft "Microsoft Knowledge Base Article - Q278887". 11 Oct. 2002
http://support.microsoft.com/default.aspx?scid=KB;EN-US;q278887& (3 Nov. 2002)

Yahoo! "How do I edit proxy/firewall preferences?"
http://help.yahoo.com/help/us/mesg/use/use-17.html (3 Nov. 2002)

Microsoft "Security & Privacy for Home Users"
http://www.microsoft.com/security/home/ (3 Nov. 2002)

Howard, Dr. John D. "Policy Implications and Recommendations".
http://www.cert.org/research/JHThesis/Chapter14.html (12 Oct. 2002)