Global Information Assurance Certification Paper

Security In-Depth for Home-based Networks with an "Always-on" Internet Connection

David Gibson
GSEC Practical Assignment version 1.4b
November 20, 2002

Abstract

In our society of ever increasing technology, it is not uncommon for there to be as many (or more) computers in a given household than there are users. Combine this with the proliferation of high-speed, always-on internet connections and you have a surge in the number of homes with small peer-to-peer networks that are attached to the internet. Many of these small networks have been assembled simply to provide for sharing the coveted internet connection as well as for file and printer sharing. A problem arises because by default these networks and computer systems are not configured for security.

The solution to this problem lies in a layered security model. This "Security in Depth" is composed of a number of low cost (and generally easy to configure) building blocks. These security building blocks can be grouped into three categories. The first is hardware issues which covers hardware-based firewall/router combinations. The second is software issues which covers personal firewalls, anti-virus software, software patches, and basic system configurations. The third category is user issues which covers some areas where basic user education will yield a more secure environment.

Security In-Depth for Home-based Networks with an "Always-on" Internet Connection

David Gibson
GSEC Practical Assignment version 1.4b
November 20, 2002

Introduction

In our society of ever increasing technology, it is not uncommon for there to be as many (or more) computers in a given household than there are users. Combine this with the proliferation of high-speed, always-on Internet connections and you have a surge in the number of homes with small peer-to-peer networks that are attached to the Internet. Many of these small networks have been assembled simply to provide for sharing the coveted Internet connection as well as for file and printer sharing. A problem arises because by default these networks and computer systems are not configured for security. Often times they are built for ease of use by the end user. Computers often have no passwords or very simple passwords, and file sharing is wide open with no security constraints. The "everyone has access to everything" mode just doesn't work in the world of the Internet.

Add to this an increasingly complex threat from just about all directions. In an article published in Spring 2002[i], a writer from the Symantec Corporation discusses blended threats. These threats are set apart by five unique characteristics:

- Cause harm
- Use multiple attack methods
- Require no user action to trigger (automated)
- Exploit known vulnerabilities
- Have multiple propagation techniques

The solution to this problem lies in a layered security model. This "Security in Depth" is composed of a number of low cost (and generally easy to configure) building blocks. These security building blocks can be grouped into three categories: hardware issues, software issues, and user issues. The main hardware issue that I will discuss is the use of a hardware-based firewall/router combination to provide a first line of defense. The software issues I will cover are software-based personal firewalls, anti-virus software, operating system and other application patches, as well as some basic system configurations that will enhance the level of security. The third category is user issues. User issues cover areas where a little knowledge can go a long way toward eliminating risky computing behavior that can defeat even the most securely designed and built network.

When it comes right down to it, the average home user, even one with a fairly sophisticated network configuration, doesn't have the time or desire to work for hours each week to keep there systems secure. The purpose of this document is to lay out an easily implemented and maintained layered security solution that will yield results against many of the threats associated with a private home-based LAN attached to the internet.

Hardware Issues

Since the scope of this project deals with securing small home based networks that are connected to the internet, I will not be discussing any of the larger (and more expensive) hardware based security options that would be employed by businesses and other larger network installations.

Combination Firewall Router

The point where the local area network (LAN) meets the internet is called the perimeter[ii]. The main hardware based security building block that I will discuss is designed to protect the perimeter, or to be the first line of defense at the perimeter. This building block is a combination router and firewall. Like the sentry at the gate of a military installation, who directs traffic and only allows those to pass that have proper credentials; a broadband router with a built in stateful packet inspection firewall provides a first line of defense at the perimeter of the LAN. These combination router/firewalls provide the following benefits:

- Network Address Translation – NAT is a method to hide the IP addresses of a private network from the Internet while allowing the computers on that network to access the resources of the Internet. NAT allows multiple computers to use a single IP address[iii].
- Stateful Packet Inspection – SPI provides protection against a number of Internet threats such as; Ping of Death, SYN Flood, Land Attacks, IP Spoofing, and Other DoS (Denial of Service) Attacks.

Configuration is usually through a web interface, and is fairly simple. There are a couple of settings that are important to configure properly for a secure setup. First, change the default administrative password. This is a good candidate for a complex password. Second, there is usually a setting that will allow access to the configuration interface from the Internet facing interface. This needs to be disabled. The table below contains vendor links for a number of popular firewall router combinations.

Firewall/Router Products

Product	Vendor Link
D-Link Express EtherNetwork™ 4-Port Ethernet Broadband Router – DI-604	http://www.dlink.com/products/broadband/di604/
Hawking Dual WAN Firewall Router with 4-Port Switch – FR24	http://www.hawkingtech.com/prodSpec.php?ProdID=101
Linksys Broadband™ EtherFast®Cable/DSL Firewall Router - BEFSX41	http://www.linksys.com/products/product.asp?prid=433&grid=23
Netgear ProSafe Firewall Router – FR114P	http://www.netgear.com/products/details/FR114P.asp
SMC Barricade Cable/DSL Broadband Router – SMC7004VBR	http://www.smc.com/index.cfm?sec=Products&pg=Product-Details&prod=257&site=c

PC Magazine published a comparison and review of five different firewall routers dated October 23, 2002[iv]. All of the firewall routers that were reviewed have slightly different sets of features; so a bit of homework will be required to select the best unit for a specific application. This review provides a lot of good information that will help make that decision easier.

Software Issues

Personal Firewalls

The next layer in our security model is a software-based personal firewall. Personal firewalls are installed on each computer in the network and should track both incoming and outgoing traffic[v]. When the firewall detects suspicious inbound IP traffic, it can block it and notify the user (usually by making a log entry). Rules also can be set that govern which applications on the computer can establish a connection to the Internet. When outbound traffic is detected that doesn't fit any of the existing rules, the user is asked if they wish to allow it. The user then can decide if the traffic is legitimate and should be allowed.

The installation process of a personal firewall can be simple. Generally a wizard will walk the user step by step through the installation. Any time that an undefined application (meaning any application without an established firewall rule) attempts to access the Internet, the firewall will display a prompt for the user to allow or deny the connection to the Internet. The most common applications

that need to be allowed to make a connection to the internet are for e-mail, web surfing, and chatting. A personal firewall will provide protection against a wide range of malware. A properly configured and used personal firewall will help to protect against falling prey to people trying to compromise your system as well as stealing your personal information. The table below contains vendor links for a few of the many available personal firewall products.

Personal Firewall Products

Product	Vendor Link
Zone Alarm	http://www.zonelabs.com
Norton Personal Firewall 2003	http://www.symantec.com/sabu/nis/npf/
Mcafee Personal Firewall	http://www.mcafee.com/myapps/firewall/default.asp?duration=2
Tiny Personal Firewall 4.0	http://www.tinysoftware.com/home/tiny2?la=EN
Kerio Personal Firewall 2	http://www.kerio.com/us/kpf_home.html
Sygate Personal Firewall 5.0	http://soho.sygate.com/products/shield_ov.htm

PC Magazine published a comparison and review of six different personal firewall products dated November 19, 2002[vi]. As with many things there appears to be some trade off between ease of use and support and the price of the packages. In the reviews the free products usually suffered in these areas.

Anti-Virus Software

No discussion of computer security would be complete without spending some time talking about anti-virus software.

The word "virus" has become a generic term for several different types of malicious programs. Most "viruses" fall into three categories; true viruses, worms, and Trojan horses. A true virus is a small program that attaches itself to another legitimate program and then replicates itself within a system when the infected program runs. Worms are programs that can spread from machine to machine by itself. One of the most common ways for a worm to spread is through email. A worm could send a copy of itself to everyone in your address book. This method of replication has brought entire email systems to a halt. A Trojan horse is a program that appears to be legitimate, but it contains a malicious program. A good anti-virus program will offer protection from viruses, worms, and Trojans horses[vii].

It used to be that if you practiced safe computing habits (some of these safe computing habits will be discussed later in the section on User Issues), you were relatively safe from viruses. Now, everyone needs virus protection. You can be a

safe computer user and still become the victim of the latest piece of malware spreading around the world. Fortunately, a properly installed and configured anti-virus package can provide another layer of security for your system.

Most anti-virus software uses two main methods of identifying viruses, worms, and Trojan horses. The first, and most reliable, detection method uses virus signatures. The anti-virus program looks for the unique pattern or signature in the files that are scanned. If it finds a match, the program knows the exact virus it has found and will alert the user and possibly try to remove the virus. The second detection method uses heuristics to identify virus-like behavior. Although the use of heuristics is less reliable than virus signatures, it is important because there is always some delay between the time a new virus is introduced to the computing world and the time the anti-virus vendors can release updated virus definition files.

Updating the virus definition files regularly is critical to maintaining a secure environment. These files contain the signatures of all the viruses, worms, and Trojan horses that have been found and dissected. The anti-virus vendors update these files as quickly as possible when they identify new viruses. It is important to get these updated files copied to each system that is running the anti-virus software in a timely (and regular) manner. Generally the anti-virus package will have a method for automatically updating these files. These updates should be scheduled at least weekly.

Another task that needs to be performed regularly is a full system scan. During regular system use, the anti-virus software is scanning the files on the computer as they are being accessed. While the on-access scan is great for detecting infected files, it is limited to files that you are actually using. An infected file may sit dormant on the system waiting for the unsuspecting user to activate the virus it contains. This is why it is important to regularly schedule a complete scan of the entire system. This can generally be done on a weekly basis.

The table below contains vendor links for a few of the available anti-virus packages.

Anti-Virus Products

Product	Vendor Link
AVG 6.0 Professional	http://www.grisoft.com/
Command Antivirus	http://www.commandsoftware.com/
eTrust EZ Armor Suite	http://www.my-etrust.com/
F-Secure Anti-Virus Personal Edition	http://www.f-secure.com/
Kaspersky Anti-Virus Personal	http://www.kaspersky.com/
McAfee VirusScan 6.0	http://www.mcafee-at-home.com/
Norman Virus Control 5.2	http://www.norman.com/
Norton AntiVirus 2002	http://www.symantec.com/
Panda Antivirus Platinum 6.0	http://www.pandasecurity.com/
Trend PC-cillin 2002	http://www.antivirus.com/

PC Magazine published a comparison and review of ten different anti-virus packages dated June 11, 2002[viii]. One side note concerning most of these products; most anti-virus packages require a subscription to maintain access to the virus definition file updates. These subscriptions are reasonably priced considering the importance of having current virus signatures.

Operating System and Other Application Patches

Most software vendors need to occasionally release software updates and patches. Sometimes these patches are necessitated by the discovery of a new vulnerability that would allow an attacker to exploit a weakness in your system. Due to the complexity of modern operating systems and other software packages (particularly office products), it seems that new vulnerabilities are being found almost daily. Exploiting a known vulnerability becomes the low hanging fruit that many hackers are looking for.

Periodically checking for updates and patches for the operating system and other major software packages is imperative[ix]. You may have to visit some vendors' Web sites looking for patches. Others provide free newsletters or bulletins that are used to keep users informed of new product updates and patches. If you are using current Microsoft Windows products, Windows Update is available as a source of the latest updates (http://windowsupdate.microsoft.com/). Microsoft also has developed an agent (available through Windows Update) that informs the user when "critical updates" are available. There are also tools available that can be used to assess the patch level of a given system. Microsoft's HFNetChk enables a person to check the patch status of Windows NT 4.0, Windows 2000, and Windows XP machines.

If you use Microsoft Office products, updates are available from the MS Office product website (http://office.microsoft.com/ProductUpdates/default.aspx). One of the best sources for other Microsoft application patches and fixes is Microsoft TechNet (www.microsoft.com/technet).

Basic System Configurations

When working to configure a secure system you will have to make some trade-offs. The more features and options that you install, the greater the risk of falling prey to some exploited vulnerability. In a home environment, only the user can decide which features are truly needed. As one support professional said, "the only way to be completely secure is not to take the computer out of the box."[x]

For the purpose of this document, I want to focus on a few of the basic system configuration settings that appear on just about every security checklist.

File and Printer Sharing

The first thing that many security checklists say to do for systems using Microsoft OS's is to disable file and printer sharing. If you don't need file and printer sharing this is a very good idea. However, many home network users want to be able to share files and printers between the systems on their local network. In my house, being able to share the "good printer" is particularly important.

While doing the research for this document, I came upon the answer to this problem. It takes a little more technical understanding, but it is not too bad. The problem with Microsoft's file and printer sharing is in the "bindings". Steve Gibson, of Gibson Research Corporation, explains that the Microsoft default is to bind all of the network adapters to all of the transport protocols, and to bind all of the transport protocols to all of the network services[xi]. His solution is to use the TCP/IP transport protocol for Internet access (i.e., bind TCP/IP to the network adapter(s) that are used to access the internet, with NO bindings to any network services), and use a safe transport protocol (unroutable NetBEUI) for all of your local Microsoft Network Services (i.e., file and printer sharing). Since NetBEUI is a local transport protocol only it will not travel beyond the first router/firewall.

For the complete description of how to configure this network setup please visit Steve Gibson's website at http://grc.com/su-bondage.htm.

Do Not Hide File Extensions of Known File Types

By default, Microsoft Windows operating systems hide the known file extensions. This feature can be used to disguise malicious programs as some other file type. For example, a malicious program named "benign.txt.exe" is displayed as "benign.txt". This makes it easier to trick a user into attempting to open the file and inadvertently running the malicious program. The importance of this configuration setting is tied to the safe computing habits and user education that will be discussed more fully in the User Issues section of this document.

There have been a number of viruses, spread by email, that are known to exploit hidden file extensions. The first major attack incorporating file extension obfuscation was the VBS/LoveLetter worm which contained an email attachment named "LOVE-LETTER-FOR-YOU.TXT.vbs"[xii]. Complete instructions for changing this setting can be found at the following link: http://www.cert.org/incident_notes/IN-2000-07.html.

Internet Browser

As was stated earlier, sometimes you have to choose security over functionality or convenience. In this section I will focus mainly on settings related to Microsoft's Internet Explorer since this is arguably the most common browser used on the home pc. The most common suggestion for configuring MS Internet Explorer given on many security "checklists" is to disable ActiveX, but there are really many more options that should be thought through to get the correct mix of security and functionality.

MS Internet Explorer has a great deal of flexibility built in when it comes to configuring it for security and privacy. One of the ways that Internet Explorer can be configured in order to reduce the loss of functionality is set up different security settings for different groups of sites. This is accomplished through the use of Internet Explorer security zones. Internet Explorer has four zones; Internet, Local Intranet, Trusted Sites, and Restricted Sites. Each security zone is configured to offer a different balance of security vs. functionality depending on the level of trust that we have for each group or classification of websites. This way we have full access to all of the features on sites that we are confident that can be trusted, and, at the same time reduce the risk from unknown or untrusted sites.

The Internet Zone is the default zone. It consists of the all sites are not specifically included in the other zones. This zone should be configured to be relatively restrictive since these sites are generally untrusted (not necessarily malicious, but untrusted). The default security setting for this zone is "Medium". The Local Intranet Zone is used for sites that are in your local computer or on your local network servers. The default security setting for this zone is "Medium Low". The Trusted Sites Zone is for sites that are highly trusted. This zone is used when minimal security is needed for a site with active content. Trusted sites must be specifically added to this zone to be used. The default security setting for this zone is "Low". The Restricted Sites Zone is for sites that are believed to contain hostile code, but that you may need to visit anyway. Sites must be specifically added to this zone. The default security setting for this zone is "High"[xiii].

For each of the zones the security level can be set to Low (most trusted), Medium-low, Medium, or High (least trusted). There is also the option to create a custom level if you want to change any security settings manually. Most of the

settings configurable in the custom security level offer three choices; Disable, Enable, and Prompt. The option to prompt the user may be useful in some environments to allow the user to decide to allow something or not, however this has at least two drawbacks. First the number of popup windows can be annoying, and second, it requires a higher level of knowledge from the user. It is for the second reason that using the "Prompt" configuration for security settings should be limited. The following link contains one of the more comprehensive lists of suggested security settings for each zone: http://www.theguardianangel.com/tutorials/browser_security_tutorials_summary.htm. I have one caveat concerning these settings; they tend to generate a considerable number of prompts, and therefore may not be appropriate for all users. A more simplified (and more restrictive) configuration can be found at: http://www.cert.org/tech_tips/malicious_code_FAQ.html.

Due to the complex nature and the number of possible security settings, ensuring that everything is configured correctly may seem like a daunting task. However, there are a number of free tools available to scan your system for possible weaknesses. I was able to locate three with only 30 seconds of searching. The following table contains links to these three tools. Since each tool looks at things a little differently, a good suggestion might be to use more than one tool and compare the results.

Free Configuration Checking Tools

Product	Vendor Link
Qualys's Free Browser Checkup	http://browsercheck.qualys.com
Symantec Security Check	http://security2.norton.com/ssc/home.asp
Microsoft Baseline Security Analyzer	http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/Tools/MBSAhome.asp

E-mail Client

The e-mail client used is another source of possible security concern. How this program is configured can make a large difference in your overall system security. Once again I will focus on the Microsoft Outlook (and Outlook Express) e-mail client due to its large install base in the home pc market. The Microsoft Outlook e-mail client is vulnerable through its use of HTML and embedded scripting such as ActiveX and Java.

Outlook uses the same security zones that are in the Internet Explorer. These zones are used to govern how HTML-based e-mail behaves. Outlook should be configured to use the "Restricted Sites" since you have very little control over who sends you e-mail.

Applying the latest security patches from Microsoft is highly recommended. The following link discusses in detail the security enhancements contained in the

Microsoft Outlook E-mail Security Update:
http://office.microsoft.com/Downloads/2000/Out2ksec.aspx.

User Issues

The topics discussed in the following sections, are just as important as (if not more than) any of the topics previously discussed in this document. They are, however, often overlooked. They are not things that can generally be configured on the computer system because they deal with the users. If a user is not properly educated in secure computer usage they become the weakest link, and the system becomes more vulnerable.

Passwords

Passwords are often considered your first line of defense when protecting your computer and the information that it holds. The basic suggestions for good strong passwords are that they should be at least 8-12 characters long, and consist of upper case letters, lower case letters, numbers, and special characters (usually punctuation marks and other non-alpha-numeric characters on the keyboard). Some of the best complex passwords (that are also easy to remember) can be developed by picking the first letter from each word of a phrase that is meaningful to you. Your password becomes really a "pass phrase." Add a couple of numbers and/or special characters and you have a strong password that will be easy to remember. ("Do you know the way to San Jose?" could become “DYKtw2SJ?”)

Once you have developed a good strong password, you have to change it. It is important to not use the same password for everything. This especially goes for internet accounts. You have no control over how the various websites secure their information. If one site were compromised, you do not want the hacker to have access to the rest of your personal information. It is also important to change your passwords regularly (every 30-60 days is common). As computer speeds have increased, the time it takes for a brute force password crack has decreased. Even with this change it is better to have a strong password for a longer duration than a week password for a relatively short time.

Downloads and Data Sharing

The key to downloaded files and shared data is simple. Treat all downloaded programs and files, e-mail attachments, and even the floppy disk your friend brought over (archaic, I know, but it still happens), as if it had been exposed to the plague. Always scan everything in this category for viruses, and be very sure that your virus definitions are current. If you don’t know what a program does, don’t run it. Just because it comes from a “friendly” source doesn’t mean that it is safe. E-mail worms replicate by sending themselves to entries in the address book on the infected system. And the advent of macro viruses means that Word documents and Excel spreadsheets can deliver a nasty payload. It all comes down to the fact that you can not assume that the file is safe.

Social Engineering

Social engineering can be regarded as "people hacking"[xiv]. Social engineering is basically when a hacker pits their knowledge and wits against another person in order to obtain passwords or other useful information. In the business world this can take a number of forms, but for home users the classic example is a hacker making a call to the user pretending to be an ISP support person working on a system problem. The phony "support person" will claim that they need the user's password to do some troubleshooting. It is human nature to want to be of assistance, but the truth of the matter is that a real support person should NEVER ask for a user's password. Once a potential hacker has your password they have access to your email, your financial records, or whatever system and data was supposed to be protected by that password.

In this era when identity theft is a growing problem, it is good practice to not give personal information out over the phone unless you are absolutely certain of the identity of the person you are talking to. The policy in my home is that we do not deal with telemarketers. They can send a sales package to me in the US mail (mail fraud is a crime that can be more easily prosecuted) and if I am interested I will contact them. I have found that this gives me an easy out of most of the annoying telemarketing calls as well as helping to protect my family's privacy.

Data Back Ups

The most important thing for all users to learn about data protection is that no matter how well protected your system is, back up your data regularly. From the security perspective, this is the last layer of our defense in depth model. A good backup not only protects your data from being damaged or destroyed by a malicious hacker or the latest virus from the internet; your data is also protected from many more mundane threats.

Computers can be stolen or vandalized. Fire, water, and power problems are hard on computer equipment. And, let's face it, sometimes hardware fails. The most common threat, however, to your data is simple user error. ("If I had a dollar for every time a user accidentally deleted a file by mistake, I would have a much larger bank account than I do.") When you are faced with missing, damaged, or corrupted data files, the easiest, and sometimes only, way to repair the damage is from a data backup.

When looking at back up options, one of the first things that must be determined is how much data needs to be backed up. For this discussion, I am only interested in the data on your system. The operating system and applications do not really need to be backed up because they can be reinstalled without great difficulty. What needs to be backed up regularly is the data only. These are the fruits of your labor, your Word documents, your Excel spreadsheets, the important data files from your favorite programs like TurboTax or Quicken, and any other files that you feel are important enough to take the time to back up.

A tip that will make backing up your data simpler is to keep your data organized in folders and subfolders in one place. Microsoft Office products generally default to saving documents in the "My Documents" folder, and you might consider using subfolders inside of this folder as a place to organize and save your work. It does not particularly matter where you save your data, but if you organize it in a way that is easy to find (and not intermixed with the application files), your back ups will be easier and more complete. There is very little worse than the feeling you get when you discover that the one file you really needed from your back up archive is not there.

The next question is to determine how often you need to perform the back up. The answer to this question depends on often you make changes to your data and how critical the data is. If you work on you system everyday, and are frequently adding, changing or deleting data, then you may need to back up the data daily. Or you may decide that a full back up once a week is sufficient. If the data on your system is less important and you create new documents only occasionally, then you might feel that a monthly back up is enough for your situation.

There are a number of different methods of backing up your data and even more types of media to use for your back up. What is important is to use a method and media that you are comfortable with. For home use, I simply burn a CD copy of my important files at regularly scheduled intervals. CD-R media is cheap, they have sufficient capacity, and the files are easy to retrieve if needed.

The last part of a good back up plan is the storage location for the back up media. If your home was damaged by a fire, and your computer was destroyed, your regular back up would be worthless if it was sitting on top of the case of your pc. The media containing important backed up files should be kept in a safe place removed from your system. The more critical that the data is, the farther away your media storage site should be. This way one disaster is unlikely to take out both your system and the back up. You may want to consider storing your important back up media with your important paper documents, in a fireproof and waterproof safe.

At the risk of repeating myself, the details of your specific choices at to back up strategy, back up software, back up media, etc., are not particularly important. What is important is that you have a reliable back up of important data. For a plain English discussion on some of the back up options, you can read the following article: http://www.pcnineoneone.com/howto/backup1.html.

Conclusion

The purpose of this document has been discuss some of the details of how to implement a layered security model that will provide "Security in Depth" for a small home network with an "always-on" internet connection. This discussion

was broken down into three major sections; Hardware Issues, Software Issues, and User Issues.

The hardware issues section was relatively small but important. We started at the perimeter and looked at hardware-based firewall/routers that provide the first line of defense with NAT (Network Address Translation) and SPI (Stateful Packet Inspection).

In the software issues section we started by discussing software-based personal firewalls that provide additional security by examining both inbound and outbound traffic. The next layer of our security model was the use of anti-virus software. The importance of keeping the virus definitions current was shown to be particularly critical as viruses and worms are released on the internet with ever increasing complexity and capabilities. This was followed by a short discussion on the importance of keeping the operating system and major applications patched as security vulnerabilities are found. The last part of this section was devoted to some basic system configurations. These included File and Printer Sharing, Hidden filename Extensions, the Internet Browser, and the E-mail Client.

The user issues section discussed areas of user behavior that can be made more secure with a little education (and maybe some nagging as well). The areas discussed include good password rules, working with downloads and data sharing, the dangers associated social engineering, and the importance of a good data back up process.

If all of these building blocks are properly configured and put in place, a secure, multi-layered defense will have been built to protect the home network. The convenience of the "always-on" internet connection can be safely enjoyed with the threats associated with that connection mitigated.

References

[i] Software Spectrum: "Constructing a Defense Against Blended Threats" Spring 2002. URL:http://www.softwarespectrum.com/intouch/edition25/symantec.htm

[ii] SecurityFocus Online: "Securing Privacy, Part One: Hardware Issues" by Scott Granneman, April 11, 2002. URL:http://online.securityfocus.com/infocus/1568

[iii] Carnegie Mellon, Software Engineering Institute, CERT Coordination Center: "Home Network Security" December 5, 2001. URL:http://www.cert.org/tech_tips/home_networks.html

[iv] PC Magazine: “Editor’s Choice: Hardware Firewalls” October 23, 2002. URL:http://www.pcmag.com/article2/0,4149,646316,00.asp

[v] SecurityFocus Online: “Securing Privacy, Part Two: Software Issues” by Scott Granneman, April 25, 2002. URL:http://online.securityfocus.com/infocus/1573

[vi] PC Magazine: “Editor’s Choice: Software Firewall” November 19, 2002. URL:http://www.pcmag.com/article2/0,4149,646315,00.asp

[vii] PC Magazine: “Personal Antivirus” by Larry Seltzer, June 11, 2002. URL:http://www.pcmag.com/article2/0,4149,7309,00.asp

[viii] PC Magazine: “Editor’s Choice: Personal Antivirus” June 11, 2002. URL:http://www.pcmag.com/article2/0,4149,11949,00.asp

[ix] Microsoft: “Keep Software Up-to-Date” April 2, 2002. URL:http://www.microsoft.com/security/articles/update.asp

[x] Microsoft: “Check Your Settings” April 2, 2002. URL:http://www.microsoft.com/security/articles/settings.asp

[xi] Gibson Research Corporation: “Shields Up: Network Bondage” by Steve Gibson, October 20, 2001. URL:http://grc.com/su-bondage.htm

[xii] Carnegie Mellon, Software Engineering Institute, CERT Coordination Center: “Exploitation of Hidden File Extensions” December 5, 2001. URL:http://www.cert.org/incident_notes/IN-2000-07.html

[xiii] TheGuardianAngel.com: “Browser Security Tutorials” November 29, 2001. URL:http://www.theguardianangel.com/tutorials/browser_security_tutorials_ie5_zones.htm

[xiv] VIGILANTe.com: “Social Engineering”, 2002. URL:http://www.vigilante.com/inetsecurity/socialengineering.htm