CABLE MODEM INTERNET ACCESS AND HOME NETWORK SECURITY

Lorelei Kaiser

GSEC Version 1.3
April 2, 2002

I. Introduction

I am writing this paper in an attempt to educate home users in the multiple risks involved in connecting their home networks to the Internet. My intent is to give home users a better understanding of how Internet communication works, the threats that will be encountered when connected to the Internet, and the security measures that need to be taken to reduce their vulnerability and to protect their network and personal data.

Cable modem Internet connectivity is a connection method that enables home users to connect multiple computers in a local network to the Internet using one Internet access point. While this is a practical method of allowing multiple users Internet access, it is also a vulnerable method. A home network is convenient and secure, until you combine that network with a connection to the worldwide Internet.

II. Internet Communication Requires TCP/IP

Communication over the Internet is accomplished through the use of the Transmission Control Protocol/Internet Protocol (TCP/IP). TCP/IP is a routable protocol that was originally designed by the U.S. Department of Defense (DOD) research project to connect multiple networks designed by different vendors for the purpose of maintaining communication links and data transfer between their five-site, wide-area network in the event of an atomic/nuclear war. TCP/IP has since emerged into the foundation of the worldwide Internet.

TCP/IP is the Internet protocol that enables access to information found at thousands of locations around the world. To connect to the Internet, you must have a unique registered public IP address. TCP is a connection-based protocol that requires the establishment of a session before data is transmitted between two machines. IP is responsible for moving packets of data from machine to machine. IP forwards each packet based on its unique IP address. TCP is designed to verify that all packets sent by a machine are received on the other end. Data can get lost during transit across the network. TCP adds support to detect errors or lost data and to retransmit packets until the data is correctly and completely received. TCP packets are delivered to sockets or ports. To identify the location and the application to which data packets need to be sent, the IP address (location) and the port number (application) are combined into one address called a socket.

Sockets are how application processes communicate with the TCP/IP protocol. Sockets define how to use the transport protocols and how to transfer data between two machines. A socket is the endpoint of a two-way communication channel. By connecting two sockets together you can pass data between processes on different computers. Sockets uniquely address packets destined for a particular application on another machine, creating a unique communication path between two machines.

When you access a web site, you are attempting to connect and communicate with a web server. A socket is created that includes the IP address of the web server and the port number that you want to connect to on that particular server. The TCP/IP transmitted data packets will include your IP address, the web server's IP address, the protocol being used, the packet number, and the data being sent (including socket information). The TCP layer will begin the establishment of your session and wait for verification from the web server that communication is accepted. On the web server side, a server socket is bound to a particular port which is listening for incoming connection attempts. When it detects a connection, the web server responds by accepting or denying the connection. Upon acceptance, a socket is created between your computer system and the web server. IP then begins routing packets back and forth for your communication. TCP will verify that all packets are transmitted until they are correctly and completely received.

To communicate over the Internet, your computer system requires the TCP/IP protocol and a unique registered public IP address. Without this information, access to the Internet will be denied.

III. Home Users and Home Network Internet Connectivity

The worldwide Internet is easily accessible to anyone with a computer and a network connection. Many home users today use their computers for personal record keeping and to document and store highly personal, confidential data. Many home users also own more than one computer and have networked their computer systems together to share resources such as files and printers. A home network is convenient and secure, until you combine that network with a connection to the worldwide Internet. Connecting your home computer network to the Internet exposes you to malicious hackers who use many different tools and techniques to exploit vulnerabilities that exist within networks and computer systems connected to the Internet. If given the opportunity, hackers can steal or destroy your confidential data, steal your identity, infect your computer systems with viruses or Trojan horse programs, and use your computer to launch attacks on other Internet users or Web sites.

Home users generally connect to the Internet through the use of an Internet Service Provider either using a dial-up connection or a cable modem connection. With either method of connection, your computer will be assigned a unique public IP address for communication over the Internet. When using a dial-up Internet connection, you are connected to the Internet only for the duration of your dial-up session. The next time you dial into the provider, you will receive an entirely different IP address. When using a cable modem Internet connection, you are connected to the Internet whenever your computer is powered on. You do not need to dial a connection or access a web site through your browser to connect to the Internet. Your IP address is assigned by the cable modem service provider and is either a DHCP leased address, which may change every couple of days, or a static IP address that will never change. Because your computer is connected to the Internet from the time you turn it on until the time you turn it off (some users leave their computers on all day) and because your IP address does not change often (if at all), hackers have more opportunity to successfully exploit any vulnerabilities that may exist in your network or computer systems. To provide an increase in your network security and a decrease in vulnerability, always power off your computer systems when you are not using your Internet connection. While a cable modem connection to the Internet has more advantages than a dial-up connection, cable modem connectivity introduces many more security challenges for the home user.

IV. Home Networks and a Cable Modem Internet Connection

The CERT/CC (Computer Emergency Response Team Coordination Center) released an Advisory in July 2001 on the "Continuing Threats to Home Users". The Advisory indicated that there had been a significant increase in activity resulting in compromises of home user's computer systems, especially when a home user accessed the Internet through a cable modem connection. CERT indicated that, in many cases, an intruder would later use compromised computer systems to launch attacks against other users or organizations. Reports at that time also showed an increase in worms targeted at home users. CERT attributed that increase to the fact that intruders know that home users are generally not equipped to defend against attacks. Many home users do not keep their computers up to date with security patches and updates, they do not run anti-virus software with current virus definitions, and they generally are not cautious when handling email attachments. CERT urged home users to take protective measures to secure their computer systems, to patch vulnerabilities that may exist, and to take the appropriate steps to recover compromised systems.

When you access the Internet through a cable modem service provider, your computer is, in effect, connected to a Local Area Network (LAN) hub. Cable modem service consists of fiber coaxial neighborhood nodes that are set up in various neighborhood locations. A fiber coaxial neighborhood node may be servicing up to two thousand cable modem users. Each cable modem user in your neighborhood is a node on the network and each user shares the same cable medium. With this type of Internet connectivity, the potential exists for users outside of your home network to 'see' the transmission of inbound and outbound data from your computer systems. Local Area Networks were designed to enable users to share resources. Cable modem access introduces vulnerability to direct computer access and entire hard drive sharing. If you keep personal information stored in the data on your computer's hard drive such as your social security number, your maiden name, your children's names, financial information, credit card information, online stock or mutual fund information, or online banking information, you must take immediate action to secure your network and protect your data. Discovery of your confidential information by an intruder with malicious intent exposes you to vulnerabilities such as loss of data, financial theft, or the possibility of identity theft.

A broadband cable modem connection is a direct connection to the Internet. If your computer is powered on, your computer is 'visible' on the Internet. While you are connected to the Internet, you have access to resources located on computers anywhere in the world. This also means that users anywhere in the world have access to resources on your computer. This type of direct Internet connection provides hackers more opportunity to attack your computer systems and increases your vulnerability to common exploits and intrusions including packet sniffing, unprotected Windows shares and chat clients, mobile code, cross-site scripting, email spoofing, email borne viruses, denial-of-service attacks, Trojan horse programs, and back door or remote administration programs that enable hijacking of your computer for the purpose of attacking other computer systems. Without your knowledge, your computer may be used to attack other Internet users or corporate organizations, creating further vulnerability to liability lawsuits for damages caused by your system. You may have legal recourse but only if you can prove that you have applied defensive measures to secure your computer systems and that you periodically check for security holes and patch vulnerabilities that are discovered.

It is important for home users to be aware of the security vulnerabilities created through the use of a cable modem Internet connection. Home users need to educate themselves to better understand Internet threats and vulnerabilities and their ability to protect themselves, their networks, and their data by utilizing defense in depth. Defense in depth is the process of designing a secure network environment through the use of multiple layers of protection such as Internet firewall barriers, anti-virus software, encryption of sensitive data, and an educated awareness of safe Internet usage. Should an intrusion occur and one layer of protection fail, other layers of protection will still exist. With multiple layers of protection in place, home users will be better equipped to secure their computers and data from accidental or intentional misuse by a malicious intruder.

V. Defensive Strategies to Secure Your Home Network

A. Use a Router and Network Address Translation

Routers were designed to route TCP/IP traffic between networks. Using router technology will enable you to share the one Internet access point assigned to you by your cable modem service provider between multiple computers in your home network. The router will be connected between your home network and the Internet (the cable modem access point). The router hardware configuration will involve physically connecting your router to the broadband cable modem Internet connection and the computers in your home network to the router.

A router that supports Network Address Translation (NAT) can be the first layer of defense when designing your secure home network. NAT is a service that maps all internal addresses to one external address, a technique that effectively hides your internal computer systems from the Internet. If your router also supports the ability to block WAN requests, you will add another layer of defense to your network by hiding network ports. This feature prevents your router from responding to 'pings' and being detected by Internet users.

To communicate over the Internet, each computer is required to use a unique registered 'public' IP address. Your broadband service provider 'leases' you one unique registered public IP address for your Internet access point. You are able to 'lease' additional registered 'public' IP addresses, but you will be required to pay a monthly fee for each additional 'lease'. When using a router that supports Network Address Translation in conjunction with a private network IP addressing scheme, you are able to share the one unique registered 'public' IP address provided by your broadband service between multiple computers in your home network for Internet connectivity. Configuring your network to use a private network IP addressing scheme will, in effect, hide your local network from the Internet.

Your router will be pre-configured with a private IP address such as 192.168.1.1 for use within your local network. It will also have a registered public IP address, which will be the unique address supplied to you by your broadband service provider for your Internet connection. Unregistered private IP addresses are not routed to the Internet. When an internal computer system wants to communicate on the Internet, the router uses NAT 'masquerading' techniques to alter the source IP address within the data packets to allow Internet communication. In outgoing packets the router swaps the local computer's unregistered source IP address to that of its registered public IP address and then forwards the packets to the Internet. When packets are returned in response, the router swaps its destination registered IP address to that of the local computer's unregistered IP address and forwards the packets to the local computer.

DHCP is an Internet protocol that is used to automate the configuration of computers that use the TCP/IP protocol designed for Internet communication. DHCP can be configured to automatically assign your network computers an unregistered private IP address, subnet mask, and default gateway (the router). Your network computers will require DHCP configuration in order to obtain their IP address information from the router. The DHCP setting is found within the Configuration tab of Network properties. For each computer in your network, highlight the network card that is bound to the TCP/IP protocol and choose Properties. Click on the IP address tab and choose Obtain an IP address automatically.

Note: If your broadband service provider configured authentication of your service based on the MAC address of the network card from the computer that was used when your cable modem service was installed, you will need a router that supports MAC Address Cloning. All hardware devices (i.e. routers and network cards) have a unique MAC address that identifies them as a node on the network. If supported by your router, MAC Address Cloning will allow you to set the router's WAN port MAC address to that of the MAC address of the network card used during installation of your broadband service.

The most important step in your router configuration is to make sure that you change the default administrative password (use a strong password, no less than 8 alphanumeric characters, including upper and lower case letters) for accessing the router's administrative HTML interface.

Routers also support advanced functions such as IP Address Filtering, Port Filtering, MAC Address Filtering, IP Port Forwarding, IPSec Pass Through, Stateful Packet Inspection, Dynamic and Static Routing, and DMZ Hosting to accommodate user preferences.

Prior to configuring your router, check the vendor's web site for firmware revisions that apply to your router model. It is important to check on firmware revisions periodically. Firmware revisions are frequent and add new features, however, they often break existing functions. It is therefore critical to keep your firmware revisions up to date. Once you have completed the firmware revision on your router, if required, and the configuration of your router, you will need to reset the power on the cable modem and restart your computers so the new router settings will take effect.

While installing a router that supports Network Address Translation does add a layer of security to your network, the possibility still exists for an attacker to 'fool' NAT by accessing your network using spoofed packets. Using the defense in depth strategy of multiple layers of defense to protect your network will give you protection at other layers should an intrusion occur.

B. Unbind Windows Networking Components from TCP/IP

Successful NetBIOS attacks allow hackers to read and write to your computer. Home networks with shared resources that are running NetBIOS bound to TCP/IP are enabling hackers the ability to view, download, and upload files to their computers and to possibly replace an executable file with another one that would install a Trojan.

Prior to configuring your home network to access the Internet through your broadband Internet connection, it is critical to unbind all Windows Networking components from the TCP/IP protocol. Microsoft operating systems, by default, are installed with Windows Networking components. Microsoft binds all hardware devices, transport protocols, network clients and services to the TCP/IP protocol. If you have a home computer network configured to use File and Printer Sharing for Microsoft Networks to share resources between computer systems, and you then connect those systems to the Internet, you are also sharing your resources with users on the Internet. Windows shares create a vulnerability to your computer network because hackers commonly use freely available tools designed to search the Internet for vulnerable Windows shares.

It is possible to share resources in your home environment without sharing them out on the Internet by using the NetBEUI protocol instead of the TCP/IP protocol. To protect your shared resources, you need to completely unbind every instance of the TCP/IP protocol from the Windows Networking components. These components include Client for Microsoft Networks, Microsoft Family Logon, and File and Printer Sharing for Microsoft Networks. Once you have completely unbound the TCP/IP protocol from the Windows Networking components, your home network will be the only network that will be able to 'see' your shared resources. Your shared network resources will no longer be visible to Internet users. Not binding these components to the TCP/IP protocol effectively closes ports 137-139, preventing NetBIOS packets from entering or leaving your network.

Windows Networking utilizes port 137 (TCP and UDP) for NetBIOS Name Service, port 138 (TCP and UDP) for NetBIOS Datagram Service, and port 139 (TCP) for NetBIOS session service. Use the DOS command 'netstat' to verify that ports 137-139 have been effectively blocked by typing netstat -a at the DOS prompt.

Blocking the NetBIOS ports 137-139 effectively guards against unauthorized system access by Internet users and prevents potential intruders from gathering information such as your computer names, user names, domain names, and MAC addresses.

C. Use BlackICE Defender to Secure Your Network at the Host Level

BlackICE Defender is not a traditional "personal firewall" though it does have some personal firewall functionality. BlackICE was designed to do dynamic intrusion detection, intruder identification, and intruder blocking. Traditional firewalls are not designed to detect attacks. They are designed to be "On" or "Off" switches that monitor your network and either allow or deny traffic based on IP addresses, protocols, or ports. With a traditional firewall, if you choose to open a port for an application, anything on that port will be allowed through the firewall. If you have blocked traffic to that port, nothing will be allowed through the firewall. BlackICE adds an intrusion element to this process. If you choose to open a port for an application, the application will be allowed and BlackICE will monitor that port for possible exploits. Typical firewalls will only monitor open ports for known attacks to those ports. BlackICE will monitor all opened and closed ports for any type of attack.

BlackICE Defender uses a seven-layer protocol analysis engine designed to extensively analyze network traffic for malicious activity. BlackICE is a packet filtering firewall that uses rule-based filtering of inbound and outbound data packets to determine possible intrusions. BlackICE filters the packets and alerts you to possible malicious activity. BlackICE is able to block any suspicious inbound or outbound packets. BlackICE is also able to block transmissions on specific network ports. Hackers will often scan computers for open ports to exploit. If you are being probed on ports not normally used, there may be a hacker trying to connect to a Trojan inside of your network. BlackICE can be configured to block common ports that hackers exploit such as NetBIOS ports 137-139. The BlackICE firewall is able to detect fragmented attacks and can also detect and stop 'spoofed' packet attacks.

Even if you have a security system in place, it is important to be able to detect an attempted intrusion from a hacker who might be able to get around your security. Intrusion detection systems monitor incoming data packets, maintain history logs, and can report attempted or successful intrusions. Intrusion detection systems report on attempts that are not successful because, in tracking these attempts, you may find that you have a determined hacker who continues to return to your system in an attempt to get into your network any you will be able to block any future attempts.

BlackICE Defender offers four protection levels including Paranoid, which blocks all unsolicited inbound traffic; Nervous, which blocks most unsolicited inbound traffic; Cautious, which blocks some unsolicited inbound traffic; and Trusting, which allows inbound traffic. Setting this level to Paranoid is suggested to provide full security. The default setting is Cautious, which is a level that has been found to allow entry of the Back Orifice Trojan.

When BlackICE detects an intrusion, its role is to protect the computer from an attack. BlackICE responds to incoming traffic in one of three ways. If the traffic is safe, BlackICE allows it to enter the computer. If the traffic contains a potential attack that is not immediately threatening to your computer, BlackICE logs the event. The event is then listed in the Events tab in the local console. If the incoming traffic contains an attack that poses a direct threat to your computer, the BlackICE firewall automatically blocks the hacker's communications. The event is then logged to the local console. If you do not want BlackICE to automatically block the threatening attack, you can choose to ignore the event.

When BlackICE detects a match to any of its attack signatures in either inbound or outbound scans, probes, or actual attacks, it will alert the user by flashing the BlackICE icon in the taskbar either red, orange, or yellow, depending on the severity of the event, and the Intruder's actions will be logged. An audible alarm can be configured to sound an alert when an event has occurred.

BlackICE can be configured to collect trace evidence files, which are useful when reporting an intrusion. BlackICE captures the severity of the attack, the timestamp, the name and type of attack, the intruder's DNS name and IP address, the victim's IP address, the parameters of the attack (such as port involved), and the count. BlackICE can do reverse identification by scanning the suspected intruder to discover more information should it be required for legal purposes. It is critical to do reverse identification while the attack is in progress. Doing reverse identification later will not work as the intruder may no longer be using the same IP address used for the attack.

If BlackICE detects an attack but is not able to provide a DNS name, the only thing you can do is block the intruder. If BlackICE is able to provide a DNS name for the intruder, this information can help to locate the intruder. Use Network Solutions WHOIS server at www.networksolutions.com/cgibin/whois/whois to determine the intruder's Internet Service Provider. BlackICE has an advICE button on the control panel that can be used to get further information on an attack that has occurred. Send an email to the intruder's ISP to report the intrusion. Most ISPs usually have a mailbox such as abuse@ or security@ to receive reports. In the email provide your name, your email address, and the name of your Internet Service Provider along with any information you are able provide from the attack such as the time of the attack, the type of attack, any NetBIOS information available, and the intruder's DNS name and IP address. Along with the email message, you will need to attach BlackICE files including Attack-list.csv (lists the time and date of the attack and the parameters of the attack), Evd2002xxyy-01.enc (a 'sniffer' trace file containing part of the traffic from the attack), and the Host/www_xxx_yyy_zzz.txt file (a log of the back trace information and may contain user names and computer names). The information in these files will be helpful to security investigators. BlackICE also has a packet-logging feature for logging all network traffic if required.

It is very important that you monitor the Summary Application to determine who may be attempting to attack your system, especially if your computer shows signs of strange behavior. Informational and suspicious events do not trigger automatic protection measures. These events usually indicate automated port scans searching your computer for vulnerabilities. Attackers program port scanning software to look at all IP addresses in a particular range. All of the computers that have an IP address in that range will receive a ping on one or more ports. If you are being scanned repeatedly by the same system, this could indicate that a hacker is preparing to attack your computer. You could at this point choose to manually block the attacker. Once the attacker is blocked, it is not possible for the attacker to perform further scans on your computer system.

It is very important to keep your BlackICE Defender software up to date. There are many ways that hackers attempt to access your computer systems. Hackers scan multiple ports on your computer looking for vulnerabilities, they use port probes aimed at specific ports when looking to exploit a particular vulnerability, they use Trojan horse probes or scans to determine if you have a Trojan horse program installed on your computer system that is exploitable, they send multiple 'pings' to determine if they can connect to your computer, and they use IP address spoofing to connect to your computer while 'hiding' behind another user's IP address. BlackICE Defender includes an easy access update section for downloading updates to the program. Regular updates are issued to ensure that BlackICE can detect and stop the latest attacks. For your protection, check this section once per week.

D. Use ZoneAlarm Pro to Secure Your Network at the Application Level

The ZoneAlarm Pro firewall is a personal firewall that defends your computer at the application level by completely blocking all ports on your computer system and monitoring both incoming and outgoing application calls. ZoneAlarm uses application control to put you in control of what applications are able to connect to the Internet. When a program or program component on your computer wants to access the Internet, ZoneAlarm displays an alert screen and requires a 'yes' or 'no' answer for that program to continue. This application control allows for custom building of Internet rules. When you have given a program permission to access the Internet, ZoneAlarm 'fingerprints' all components of the application as well as the application itself to ensure that a hacker cannot plant a Trojan horse or other malicious code that masquerades as a trusted application on your computer system. ZoneAlarm allows you to add computers or networks to either a blocked or trusted zone. For your protection, if you are receiving repeat alerts regarding an event occurring from a particular source, you can add this source to the blocked zone.

When ZoneAlarm detects an intrusion, an alert will be announced and logged. Logging for each alert will include the event rating by ZoneAlarm, the date and time the event occurred, the type of event, the protocol used by the traffic that caused the event, the name of the program attempting to send or receive data, the source and destination IP addresses, whether the blocked traffic was incoming or outgoing, the action taken by ZoneAlarm on the traffic, the source and destination DNS names, and the number of times the same event triggered an alert during that session.

ZoneAlarm has an alert advisor that can be used to obtain further information about security events that have occurred on your computer. This can help you to make better decisions about those events. The alert advisor provides an overview of the event including the IP address, the port number it came in on and the port it was attempting to connect to as well as more technical information and a Whois report from Zone Labs giving you the name, address, and contact information for the intruder's Internet Service Provider.

ZoneAlarm provides malicious code protection by blocking cookies, pop-ads, and mobile code such as scripts, embedded objects, and mime objects. ZoneAlarm also provides email protection through the use of MailSafe, which is a monitoring system that prevents the spread of malicious executables and other file types through email. To prevent potential infection, MailSafe will alert you when a possible malicious file is attached to an email. You may choose to either delete the infected email or quarantine the suspicious attachment. For added protection, you are able to add file types to the MailSafe list of monitored files.

ZoneAlarm has a ‘Stop’ button to automatically lock your computer and block all inbound and outbound traffic. An automatic lock can also be enabled to block all inbound and outbound traffic after a period of computer inactivity or when your screen saver comes on. If you are downloading a large Internet file, you can custom configure ZoneAlarm to prevent the automatic lock from interfering with that download. Locking your computer after a period of inactivity is another layer of security, especially if you tend to leave your computer on when not in use.

When you first install ZoneAlarm, it is in a ‘learning mode’. You are alerted and asked permission about every application that attempts to access the Internet as well as any application that attempts to access your system from the Internet. This is a little frustrating until you are able to complete the ‘fine tuning’ process by adding all applications on your computer system that require Internet access. When ‘fine tuning’ ZoneAlarm Pro, there will be many applications (inbound and outbound) that you will not recognize. Use a good search engine and search the Internet for the application in question. Do not enable access to the Internet until you have searched the Internet and determined what the application is and what it does for your computer system. You need to know before allowing traffic either in or out of your network exactly what that traffic is doing.

ZoneAlarm Pro offers Password protection to effectively disable other users on your computer system from making any configuration changes to your personal console settings. When configuring your password protection use a strong password that is no less than 8 alphanumeric characters, including upper and lower case letters.

When your home network is connected to the Internet, your computer systems and personal data are potential targets for malicious Internet users. ZoneAlarm will protect your home network at the application level, adding another layer to your security strategy of defense in depth. ZoneAlarm is configured by default to automatically check for product updates ensuring the highest level of protection available.

E. Use Anti-Virus Software to Protect Your Data

An anti-virus software package with current virus definition files will effectively protect your computer systems from viruses, worms, Trojan horses, Java applets, ActiveX controls, malicious Word and Excel macros, and script-based and email borne viruses. Anti-virus software is designed to detect viruses by comparing various file types to a ‘signature’ file of previously discovered malicious code.

Most anti-virus programs today include an auto-protect feature that works in the background to provide continuous protection against all types of viruses. Every time you open a file, run a program, open an email attachment, or access a floppy disk or other removable media, the software will check for viruses and prevent them from infecting your computer system. Auto-protect will also protect you from viruses transmitted through the Internet by checking files you download including Java applets and ActiveX controls. For the highest level of protection, keep your auto-protect feature turned on at all times.

Anti-virus programs perform complete hard disk virus scans, which can be run manually or on a scheduled basis. Configure your anti-virus software to scan system files and boot records at startup. Schedule your anti-virus to do a complete scan of your computer hard drive including computer memory, boot record, and master boot records once per week and to scan incoming and outgoing email.

Most anti-virus programs include a LiveUpdate feature that will automatically check for new virus definitions when you are connected to the Internet. This feature will allow you to provide the highest level of protection against malicious code.

If your anti-virus software detects a virus, you can choose to automatically repair the infected file, try to repair the file and then quarantine it if the repair is not successful, or deny access to the infected file. It is not possible to repair worms. If your anti-virus software detects a worm, you will need to delete the infected file or email.

When you purchase anti-virus software, you will receive free virus definition updates for one year. When that term has expired, you will need to either upgrade your software or purchase virus definition updates for another year. The CERT at http://www.cert.org/other_sources/viruses.html#VI lists anti-virus software vendors and provides links for updates to their products including product patches and current virus definition files. If you are not using LiveUpdate, you should check your vendor weekly for the availability of new virus definition files. You should also check for any new viruses or worms that have been reported. You can check Symantec at http://www.symantec.com and McAfee at http://www.mcafee.com/anti-virus/default.asp for the latest virus threats and advisories.

With the many new variants of viruses, worms, and Trojan horses being developed and with their multiple methods of infection and spread, it is critical to the health of your computers and to the protection of your personal data to install anti-virus software on each of your network computer systems.

To further protect your data, ensure that you make regular backups of your personal files to some form of removable media. Make a boot disk on a floppy diskette in case your computer is damaged or compromised to aid in recovering from a security breach or hard drive failure. If you have access to disk imaging software, an image file of your hard drives will provide you with the highest level of data recovery.

1. Indications of Possible Virus Infection

Indications of possible virus infection include a slower running computer, longer program load times, a noisy computer disk drive, reduced memory or disk space, bad sectors on a floppy disk, unusual error messages, unusual screen activity, failed program execution, failed system boots, changes in the length of programs, changes in file date or timestamp, unexpected writes to a drive, and unexplainable files found on computer disk drives.

While installing anti-virus software will add another layer to your security strategy of defense in depth, this layer will only remain an effective layer of defense if you keep your software and virus definition files up to date.

F. Use Encryption to Secure Your Data

Email messages and other data files transmit across the Internet in clear text. If no encryption method is used, an eavesdropper using a packet ‘sniffing’ product can intercept your data packets as they travel to their destination and the clear text data within the packets will be decipherable.

Encryption software can be used to protect the confidentiality of your data by scrambling it so that other users are not able to read it and to provide integrity, authentication, and non-repudiation of your data through the use of digital key signatures.

Pretty Good Privacy (PGP) is a strong encryption product that is free for personal use. PGP can be downloaded at http://www.pgpi.org. PGP allows you to secure email messages and files. PGP uses a public and private key set to allow you to exchange secure data. For further security of your data, digital signatures can be used. When using encryption to send personal data to another user, you can be sure that the data will be received and read only by that user.

PGP uses of a pair of keys, a ‘public key’ and a ‘private key’, to ‘lock’ and ‘unlock’ your encrypted email messages or files. To use PGP, you create a public key and a private key. The public key is used to lock your data. You publish your public key by sending it to a PGP key server on the Internet. When other users want to send you a private email message or file, they use a copy of your public key from the PGP key server to lock the data before sending it to you. When you receive the data, you use your private key to unlock and read the email message or file. It is very important to remember to protect your keys. If you lose a key or forget your passphrase (password), the data you previously encrypted will remain forever encrypted and unreadable.

While the use of encryption to protect your data adds another layer to your security strategy of defense in depth, the potential still exists for a malicious eavesdropper to intercept your packets during transmission and to use freely available tools to break the encryption algorithm and decipher your data.

G. Apply System and Application Security Patches and Updates

In order to secure your computer data, it is critical for you to determine every software application that has been installed on each of the computer systems in your local network. Take an inventory of all software applications installed and document this information. It is impossible to secure your data if you are not aware of what is running on your computer systems. Every software application has the potential to create security vulnerabilities. Take your inventory list and visit the vendor site for each software application documented to check for available security patches or updates. Remember to keep your inventory list up to date. When you install a new software application, be sure to add that application to your computer software inventory list.

Microsoft provides a website called Windows Update for obtaining Microsoft product updates including updates for the Microsoft Office suite of products. This website can be found at http://windowsupdate.microsoft.com. This site contains a catalog of fixes, updates, and enhancements to Windows and many programs that work with Windows. Windows Update scans your system to see what you have installed and gives you a list of suggested available components. This system check assures that you get the most up to date and accurate versions of software downloaded from the site. Be sure to immediately download any critical updates recommended for your system. Critical updates will fix known problems such as security issues that are specific to your computer. Do the system check for both the Microsoft Windows Family and the Microsoft Office Product Updates (if you run the Microsoft Office suite). If you experience any difficulty with this process, check the Support Information for known issues regarding the Product Updates.

Many hackers make careers out of experimenting and discovering new computer exploits. With great effort and determination, they uncover new exploits every day. Meanwhile, they continue to scan millions of computers on a daily basis looking for both old and new vulnerabilities. Without dedication to educating yourself about exploits and vulnerabilities, it is unrealistic to believe that you will never be scanned or that a hacker will never find an exploitable vulnerability within your computer systems.

To protect yourself and your computer data, it is important to set a schedule for checking the availability of security patches and updates for all applications listed on your computer inventory list. You should also routinely check sites that release information on newly discovered exploits and vulnerability alerts such as the CERT Coordination Center's "Current Activity" site at http://www.cert.org/current/current_activity.html, which includes a regularly updated summary of the most frequent, high-impact types of security incidents and vulnerabilities currently being reported to the CERT/CC, and The SANS Institute's "incidents.org" site at http://www.incidents.org.

VI. Website Access Vulnerabilities

A. Active Content

Active Content is a term used for reusable program code that is embedded in the contents of web pages to produce animations, pop-up menus, interactive objects, multimedia effects, and sophisticated applications. Other terms used to describe active content are executable content, active code, and mobile code. When you access a web page using your web browser, the active content or embedded code is automatically downloaded and executed on your computer system. Java and ActiveX (active content) both embed code within the coding of HTML web pages through the use of Java applets or ActiveX controls. If active content has been poorly designed, it can enable an intruder to determine your computer and user names, to access your hard drive, to modify files, to delete files, to execute files, and to access your local network. A malicious intruder could then exploit this vulnerability for the purpose of downloading remote administrative tools to your computer.

To protect yourself from the vulnerability of active content, disable Java applets and ActiveX controls in Internet Explorer. You will find the settings to disable Java in Internet Explorer, Tools, Internet Options, Advanced tab, and Microsoft VM. Information on how to disable ActiveX controls is available at http://support.microsoft.com/default.aspx?scid=kb;EN-US;q240797.

B. Secure Sockets Layer

When you access a website, you are connecting to a web server. If the web page you are accessing is a secure web page, the security protocol Secure

Sockets Layer is used for communication between your computer, the client system, and the web server. The web server will indicate whether SSL is required for the particular web page you are accessing. If SSL is required, your computer, the client system, will negotiate with the web server to determine what type of encryption the session will use. The strongest algorithm that the two systems support will be selected. At that point encryption keys are exchanged in order to enable encrypted messages between the client and the server. Once the keys have been exchanged, all further communications between your computer and the web server will be encrypted.

Internet Explorer's default configuration of the Secure Sockets Layer protocol exposes your computer system to the possible exploit of a vulnerability that exists when accessing secure websites using SSL 2.0. There are two different versions of the Secure Sockets Layer, and they are both enabled by default during installation of Internet Explorer. The two versions include SSL 2.0, which uses DES as its encryption algorithm, and SSL 3.0, which uses 3DES as its encryption algorithm. The DES encryption algorithm has been found to be vulnerable to man-in-the-middle attacks. DES is no longer a supported encryption algorithm because it is not considered to be secure. If you leave the option for SSL 2.0 enabled within Internet Explorer, it is possible that SSL 2.0 will be used during a secure communication rather than SSL 3.0 if an SSL-enabled website has been incorrectly configured to use SSL 2.0.

You are able to determine if SSL is enabled on a web page by looking at the bottom of your browser. In Internet Explorer there will be a small icon of a lock in the lower right corner. This means that your communication is being protected with encryption; however, you are not able to determine whether SSL 2.0 or SSL 3.0 is the protocol being used for that communication.

It is important to note that using the Secure Sockets Layer does not guarantee that your data will be secure. Secure Sockets Layer only secures data as it is transmitted over the network. It is still possible for an intruder to capture data packets during transmit across the network and to then decrypt those packets. The risk of this occurring is reduced if you are using strong encryption, however, the risk still exists. Secure Sockets Layering also does not protect your data once it reaches the destination computer. If the destination computer stores your information in a public location or if an attacker gains unauthorized access to that computer, your data is still vulnerable. To protect yourself from web sites that are improperly configured, disable the use of SSL 2.0. You will find the setting to disable SSL 2.0 in Internet Explorer, Tools, Internet Options, Advanced tab, Security, and uncheck SSL 2.0.

C. Cookies

If you have cookies enabled within Internet Explorer, web servers can use cookies to store information about you when you access their web pages. When your session with the web server has been closed, the cookie downloads to your hard drive for future access by that same server. When you return to the same web server, it will access the cookie and append session information to it. This cookie is embedded in the HTML information traveling between your computer and the web server. Cookies were designed to store information about your browsing preferences, however, personal information such as user names, passwords, home addresses, and credit card numbers have also been found in cookies.

Web servers were intended to have restricted access to only cookies that were stored on your computer by that web server, however, a security hole in Internet Explorer will allow any web server to access the entire directory of cookies that have been placed on your hard drive by all other web servers. This creates a vulnerability to malicious websites stealing data that you have stored in cookies. In addition it is also possible for malicious users to access and alter the contents of the cookies. To protect yourself from this vulnerability you can block cookies that use personally identifiable information without implicit content. This setting can be found in Internet Explorer, Tools, Internet Options, and Privacy tab.

D. Browser Cache

If you use your computer for online transactions such as shopping, banking, and stock trading or mutual funds, clear your browser cache after visiting these sites. Browser cache may include the results of forms or database queries containing information such as your credit card numbers, PINs, passwords, insurance and bank details, or other private information. In the event of an intrusion, it would be possible for a hacker to download files from your browser cache and get access to your private information and online activities. To clear your browser cache, go to Internet Explorer, Tools, Internet Options, General tab, and Delete Files.

E. Spyware

Spyware is Advertising Supported software (Adware). Spyware, usually in the form of a pop-up banner, is a way for shareware authors to make money from a product. Besides being extremely annoying, these advertising banners often install tracking software on your computer system. This tracking software is designed to gather information about your browsing habits and to report that information back to a central server. Using a personal firewall such as

ZoneAlarm Pro will alert you to utilities and applications that attempt to report back to central servers and you will be able to stop that process.

VII. Malicious Code

Malicious code incidents are rising at a rapid rate. This increase is attributed to the increased use of email for communication and the many freely available virus tool kits that help intruders develop Internet worms. With the help of virus tool kits, intruders are getting more sophisticated. Intruders target software that is widely used and known to have numerous vulnerabilities. When the software has been patched, the intruder just moves on to another vulnerable application. Malicious code is no longer considered just an annoyance to an infected user, it has become a major security threat to all Internet users.

ICSA Labs, a division of TruSecure Solutions, conducts a survey each year called the "Virus Prevalence Survey" that continues to show a substantial increase in the infection rate of malicious code. This survey indicates an increase in the number of infection methods possible for malicious code, in the number of viruses and worms that spread using multiple methods of infection attempting to exploit multiple vulnerabilities, and in the number of host-based malicious code that infects and spreads through the Internet. Contributing to rising infection rates are new virus types, increased use of multiple email programs, and new methods of infection and spreading capabilities. Malicious code infection can do anything from infecting your computer with a harmless virus to allowing access to your computer and personal files to formatting your entire hard drive.

A. Viruses

Viruses are fragments of malicious code that attach themselves to computer programs, files, or boot sectors and require human intervention to spread. Program and file viruses spread to other programs or files when they are executed or opened by the infected user. Boot sector viruses write themselves to system areas of hard disks and floppy diskettes and are spread through the sharing of infected diskettes. Email borne viruses spread through email and require the user to open an infected attachment in order to become infected.

Macro viruses are embedded within word processors and spreadsheets (Word and Excel) and can execute commands to allow access to your computer and personal files. Macro viruses are memory resident viruses. They attach themselves to a system function such as FileSaveAs and remain in memory until that function is called. When the function is called, the virus obtains control and can infect again. Macros spread through the sharing of files. You can protect yourself to some extent against macro viruses by disabling AutoOpen macro, using the Word system macro DisableAutoMacros, but this is not a reliable way to stop the viruses.

Email viruses spread through the use of email by sending themselves to addresses in the infected user's address book. They are able to spread fast because people in the victim's address book have a connection to them and will usually open the email. Email viruses are embedded within the email itself. Email viruses may contain an attachment but it is not necessary for a user to open the attachment in order to become infected. Email viruses can execute even if the user only reads or previews the email. Email viruses generally target Microsoft Outlook and Outlook Express users. It is important to understand how to prevent attachments from being automatically executed by the mail client and how to recognize potentially harmful attachment types. In Outlook and Outlook Express there is a feature called "Preview Pane". When you click on an email there is an area of the screen where you can see the contents of the email. This Preview Pane actually opens the email. This is very dangerous because many email viruses will run when an email message is opened, you do not need to open an attachment to get infected. It is very important to turn off your email program's "Preview Pane". You will find instructions for turning off the Preview Pane in Microsoft Outlook and Outlook Express at http://www.apcsnh.com/vacm/previewpaneoff.html. If you can see the contents of an email when you click on it, your Preview Pane option is turned on.

1. Melissa

The Melissa virus was a macro virus that was sent in an email attachment. When the email attachment was opened, the virus checked to see if the user's computer was installed with Microsoft Outlook. If the virus found Outlook, it mailed itself to the first 50 entries in the Outlook address book. Even systems that did not spread the virus directly by email still had their Microsoft Word documents infected and continued to pass the virus on.

B. Worms

Worms are malicious programs that use security holes in computer networks to copy themselves from machine to machine across network connections. They can very quickly spread themselves to thousands of computers. Worms are not considered to be viruses because they do not require human intervention to spread. Many worms specifically target vulnerabilities in Microsoft Outlook and Outlook Express.

1. W32/Sircam

W32/Sircam was a worm that spread through email and unprotected network shares. Spreading through email required a user to open an attachment to infect the user's machine. It was possible to trick user's into opening this malicious email attachment since the file appeared without the .EXE, .BAT, .COM, .LNK, or .PIF file extensions if "Hide file extensions for known file types" was enabled in Windows. This virus mailed out random files from the infected user's hard drive as decoy mail messages containing the malicious code. W32/Sircam also copied itself to unprotected network shares, creating multiple copies of malicious code in different locations on hard drives. Spreading through network shares required no human intervention. To avoid worms such as W32/Sircam, do not hide file extensions. Instructions for allowing the viewing of file extensions are available at http://www.cert.org/incident_notes/IN-2000-07.html.

2. W32/Gibe

The CERT/CC continues to receive reports regarding a piece of malicious code that was written for Windows platforms. This code is commonly known as W32/Gibe and is a mass-mailing worm that spreads through email disguised as a Microsoft security bulletin and patch. The attached patch file is an executable and is malicious code. A user must execute the attached file in order to be infected and, when executed, the code will send itself to addresses in the victim's Microsoft Outlook address book. This is the first Internet worm to also generate email addresses from online directories. If the victim has a registered email address with Yahoo's People Search Directory or Switchboard, the worm generates a search in those public email databases for last names in which the first and third letters are random consonants, with the middle letter being a random vowel. When it hits a last name that produces several pages of results, it sends itself to those email users. Though a large list may be produced, these are people with no connection to the victim and the spread of infection will not be as fast. When W32/Gibe has successfully infected a victim, it creates a "back door" on the system on port 12378 that enables a remote attacker to take control of the victim's computer.

C. Trojan Horse Programs

A Trojan horse is a malicious program that appears to be one type of program but has a hidden malicious function. A Trojan horse may be a program that looks harmless on your screen but may be modifying or deleting files on your hard drive in the background. Trojan horse programs do not spread by making copies of themselves like worms but usually spread through email or through web page downloads. Well-known Trojan horse programs include

Back Orifice, NetBus, and SubSeven. Trojan horse programs allow hackers access to your computer systems and confidential data. Trojans often install hacking tools on your hard drive that later enable remote control of your computer. Hackers will use remote controlled computers in larger denial-of-service attacks.

D. Malware

Malware is a term that is applied to a malicious program that has the combined properties of a virus and a worm. Malware uses JavaScript, VBScript, or a macro language application to spread. Malware spreads through network connections.

Malicious intruders are going to continue to explore ways to get into your computer system. New vulnerabilities and threats are reported every day. Protect your computer and your personal files by installing an anti-virus software product. Check for updates to this product once per week and whenever new viruses have been reported.

VIII. Instant Messaging Applications

Home users often use Instant Messaging software or chat programs to communicate with friends online. Many chat programs allow the exchange of executable files. Instant messaging applications provide a mechanism for information to be transmitted between computers on the Internet including exchanged conversation, web site links, and files. Do not follow links sent you or accept incoming files from Instant Messaging users you do not know. Intruders trick unsuspecting users into downloading and executing malicious software, which allows the intruders to use the systems as attack platforms for launching distributed denial-of-service (DDoS) attacks on other Internet users.

IX. Home Users and Home Network Internet Connectivity Summary

The bottom line regarding the defense of your home computer network is that the more layers of protection you are able to provide, the more secure your network will be and the safer your computer systems and data will be from malicious intruders attempting to exploit network or computer vulnerabilities. The layers of defense described above include a router that supports Network Address Translation and Block WAN Request as a barrier between your home computer network and the Internet (effectively hiding your network), the unbinding of the Windows network components from the TCP/IP protocol (preventing file sharing with Internet users), a combination of two types of personal firewalls (one that is capable of providing intrusion detection and the other that provides application level protection), anti-virus software with current virus definition files (ensuring current protection from malicious code), encryption software (securing your data as it travels over the Internet), and operating system and application security patches and updates (ensuring current protection from newly discovered vulnerabilities).

In conclusion, I believe that by using a defense in depth strategy of multiple layers of defense you will be providing a highly effective security structure for the protection of your home network and personal data. Maintaining this level of network security will require frequent network monitoring, investigation of current threats and vulnerabilities, and the application of recommended security patches.

X. List of References

Dulaney, Emmett. TCP/IP. Indianapolis:
New Riders, September 1998.

Gilbert, Howard. “Introduction to TCP/IP.” 2 Feb 1995.
URL: http://www.yale.edu/pclt/COMM/TCPIP.HTM.

Howard, Elliotte Rusty. “Server Sockets.” Week 12: Network Programming.
April 18, 1997.
URL: http://www.ibiblio.org/javafaq/course/week12/19.html.

CERT Coordination Center. “Home Network Security.” December 5, 2001.
URL: http://www.cert.org/tech_tips/home_networks.html.

Carpenter, Jeff. Dougherty, Chad. Hernan, Shawn. “CERT Advisory CA-2001-20 Continuing Threats to Home Users.” July 23, 2001.
URL: http://www.cert.org/advisories/CA-2001-20.html.

VICOMSOFT. “22: What’s the downside to using cable access?” Cable Access Q&A – Part One. “11. What is a fiber coaxial neighborhood node?” Cable Access Q&A – Part Two.
URL:
http://www.vicomsoft.com/index.html?page=http://www.vicomsoft.com/knowledge/reference/cable.modems.html*track=internal.

Grossman, Mark. “Third Party Liability for Hacking.”
URL: http://www.ciao.gov/Audit_Summit/SummitLibrary/3rdPtyLiab4Hackg.pdf.

Linksys. Support Page For BEFSR41 Cable/DSL Router.
URL: http://www.linksys.com/support/support.asp?spid=1.

Linksys. “Advanced Features.”

URL: http://www.linksys.com/tech_helper/advanced.html.

VICOMSOFT. "Network Address Translation FAQ."
URL:
http://www.vicomsoft.com/index.html?page=http://www.vicomsoft.com/knowledge/reference/nat.html*track=internal.

Machrone, Bill. "Is Your Home LAN Secure?" October 16, 2001.
URL: http://www.pcmag.com/print_article/0,3048,a%253D14485,00.asp.

PRACTICALLY NETWORKED. "Cloning your MAC address."
URL: http://www.practicallynetworked.com/support/MAC_addr_clone.htm.

Gibson, Steve. Shields UP!! "Internet Connection Security for Windows Users." Oct 25, 2001.
URL: http://grc.com/su-rebinding9x.htm.

INTERNET|SECURITY|SYSTEMS. "Support Knowledgebase."
URL: http://advice.networkice.com/advice/Support/KB/default.htm.

Breiling, Susanna. Plato, Andrew. "BLACKICE STOPS HACKERS COLD." BlackICE Agent. Installation Guide Version 2.5. 2000.
URL: http://www.networkice.com/docs/product/BlackICE_Installation_AG_25.pdf.

INTERNET|SECURITY|SYSTEMS. "How does your product compare with personal firewalls?" Support Knowledgebase.
URL: http://advice.networkice.com/advice/Support/KB/q000025/default.htm.

Moor, Dean. "Hacking 101.2." Actrix Newsletter. October 2000.
URL: http://editor.actrix.co.nz/byarticle/hacking02.htm.

Zone Labs. "ZoneAlarm Pro 3.0 Technical Support." Service & Support
URL: http://www.zonelabs.com/services/support_3faq.htm.

Zone Labs. "ZoneAlarm Pro 3.0." Products & Solutions.
URL: http://www.zonelabs.com/products/zap.

Symantec. "Security Response."
URL: http://www.symantec.com.

McAfee. "Virus Information." Secure Your PC.
URL: http://www.mcafee.com/anti-virus/default.asp.

ICSA Labs. "Anti-Virus Product Developers Consortium."

URL: http://www.icsalabs.com/html/communities/antivirus/index.shtml.

CERT Coordination Center. “Computer Virus Resources.” March 1, 2002.
URL: http://www.cert.org/other_sources/viruses.html#VI.

“A Newcomer’s Introduction to Pretty Good Privacy (PGP).”
URL: http://www.mindspring.com/~aegreene/pgp.

Microsoft Windows Update. “Welcome to Windows Update.”
URL: http://windowsupdate.microsoft.com.

CERT Coordination Center. “CERT/CC Current Activity.” April 2, 2002.
URL: http://www.cert.org/current/current_activity.html.

Accessible Documentation for Microsoft Products. “Advanced Web Technology.” FrontPage 2000 Documentation. Chapter 11.
URL: http://www.microsoft.com/enable/download/products/office/fp2k/fp18.txt.

Microsoft Product Support Services. “How to Disable ActiveX Control in Internet Explorer (Q154036).”
URL: http://support.microsoft.com/default.aspx?scid=kb;EN-US;q154036.

Bollinger, Lloyd. “SSL Q&A.” SSL Questions and Answers.
URL: http://www.washuwebclass.org/ssl_q&a.htm.

Mayer-Schonberger, Viktor. “The Cookie Concept.”
URL: http://www.cookiecentral.com/content.phtml?area=2&id=1.

Disabatino, Jennifer. “Security hole in IE reveals data in cookies.” November 09, 2001.
URL: http://www.computerworld.com/storyba/0,4125,NAV47_STO65588,00.html.

O’Dwyer, Frank. “Microsoft Internet Explorer: Cache Vulnerability.” January 6, 1997.
URL: http://www.brd.ie/papers/mscache/mscache.html.

Spychecker. “what is spyware?”
URL: http://www.spychecker.com/spyware.html.

TruSecure. “ICSA Labs’ Annual Virus Prevalence Survey Shows Infection Rate of Malicious Code Increasing.” March 4, 2002.
URL: http://www.trusecure.com/html/news/press/2002/pravsurvey030402.shtml.

Symantec. “Guide to Malicious Code – The Invisible Enemy.” Internet security for the home.
URL: http://www.symantec.com/securitycheck/maliciouscode.html.

Virus Encyclopedia. “Macro Viruses (Word, Excel, Access, PowerPoint, Amipro, Visio).”
URL: http://www.viruslist.com/eng/viruslist.html?id=7.

Antivirus Software. “What is an email virus?” Email Help Center.
URL: http://antivirus.about.com/library/blemail.htm.

LivingInternet.com. “Script Viruses.”
URL: http://www.livinginternet.com/?i/is_vir_mac.htm.

CERT Incident Note IN-2000-07. “Exploitation of Hidden File Extensions.” July 27, 2000.
URL: http://www.cert.org/incident_notes/IN-2000-07.html.

PROLAND SOFTWARE. “Melissa Virus.”
URL: http://www.pspl.com/virus_info/w97m/melissa.htm.

King, Brian B. “W32/Gibe Malicious Code.” CERT Incident Note IN-2002-02. March 13, 2002.
URL: http://www.cert.org/incident_notes/IN-2002-02.html.

VACM Newsletter Archives. “Turn the Preview Pane Off In Your Email Program.” Virus Alerts For The Common Man. How-To: Disable Your Preview Pane Now!
URL: http://www.apcsnh.com/vacm/previewpaneoff.html.