

Connecting to the Internet Securely; Protecting Home Networks

CIAC-2324

William J. Orvis

Paul Krystosek

Jack Smith



DISCLAIMER

This document was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor the University of California nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or the University of California. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or the University of California, and shall not be used for advertising or product endorsement purposes.

This work was performed under the auspices of the U. S. Department of Energy by the University of California, Lawrence Livermore National Laboratory under Contract No. W-7405-Eng-48.

This report has been reproduced directly from the best available copy.

Available electronically at <http://www.doc.gov/bridge>

Available for a processing fee to U.S. Department of Energy

And its contractors in paper from

U.S. Department of Energy

Office of Scientific and Technical Information

P.O. Box 62

Oak Ridge, TN 37831-0062

Telephone: (865) 576-8401

Facsimile: (865) 576-5728

E-mail: reports@adonis.osti.gov

Available for the sale to the public from

U.S. Department of Commerce

National Technical Information Service

5285 Port Royal Road

Springfield, VA 22161

Telephone: (800) 553-6847

Facsimile: (703) 605-6900

E-mail: orders@ntis.fedworld.gov

Online ordering: <http://www.ntis.gov/ordering.htm>

OR

Lawrence Livermore National Laboratory

Technical Information Department's Digital Library

<http://www.llnl.gov/tid/Library.html>

TABLE OF CONTENTS

Table of Contents	i
Document Conventions.....	iv
1 Overview	1
2 Introduction.....	3
3 What's Happening In Your Home Computer?.....	5
3.1 A Conduit to the Inside of the Company Firewall.....	5
3.2 An Attack Site.....	7
3.3 A Home Spy.....	7
3.4 A Denial of Service Drone (Zombie).....	8
3.5 A Worm Breeding Ground.....	9
4 Security Risks of Home Networks.....	11
4.1 New Systems Are Not Secure.....	11
4.2 Internet Usage Habits.....	11
4.3 Changing Internet Connectivity.....	12
4.4 Sharing Systems.....	13
5 Securing Your Systems.....	15
5.1 Keep Your Systems Up-to-Date	15
5.1.1 Updating Windows Systems.....	16
5.1.2 Updating Linux Systems.....	17
5.1.3 Updating Macintosh Systems	18
5.2 Securely Configure Your System	18
5.2.1 Securely Configuring Windows.....	19
5.2.2 Securely Configuring Linux	23

5.2.3	Securely Configuring Macintosh	23
5.3	Eliminate Unneeded Services	23
5.3.1	Windows	24
5.3.2	Linux	25
5.3.3	Macintosh.....	27
5.4	Use Remote Services that Protect the Login.....	29
5.5	Use Good Passwords.....	30
5.5.1	Choosing Password Complexity	30
5.5.2	Choosing Password Length.....	32
5.5.3	Protecting the Encrypted Password	32
5.5.4	Determining When to Change Passwords.....	33
5.6	Use Current Antivirus	36
5.7	Moderate Your Internet Usage Habits	37
6	Creating an Electronic Security Perimeter	43
6.1	Security Barrier Options for Home Networking.....	43
6.1.1	Simple Packet Filtering Firewall	44
6.1.2	NAT Router	45
6.1.3	Stateful Packet Inspection Plus Port Forwarding.....	47
6.1.4	Packet Filtering	47
6.1.5	Program Authorization.....	48
6.1.6	Remote Management of Firewalls	48
6.1.7	Wireless Home Networks (WLAN).....	49
6.1.8	VPN Options	50
6.1.9	Software Firewalls	51
6.1.10	Hardware Firewalls.....	52

6.1.11	Tradeoffs	53
6.2	Protecting a Dial-up Connection.....	55
6.3	Protecting a Small Network with a Dial-up Connection	56
6.4	Protecting a Single System with a Broadband Connection	57
6.5	Protecting a Home Network With a Broadband Connection.....	58
6.6	Protecting a Home Network with Wireless Networking	58
7	Use Protected Connections Between Home and Work.....	59
8	Policy Considerations Related To Working From Home	61
8.1	Company Computer at Home	61
8.2	Personal Computer used to Access Company Resources	62
8.3	Maintaining The System	62
8.3.1	Company Owned System.....	62
8.3.2	Employee Owned System	62
8.4	Antivirus Software	63
8.5	VPN Software	63
8.6	Company Provided Firewall	63
8.7	Scanning and Testing.....	64
9	Conclusions.....	65
	Appendix A – Available Software Firewalls.....	67
	Appendix B – Available Hardware Firewalls.....	69
	Appendix C – Networked Resources for Home Networking	71
	Appendix D –Known Backdoor Ports.....	73
	Appendix E – Glossary	75

DOCUMENT CONVENTIONS

Characters you type exactly as shown are in **bold** type. This includes commands, paths, and switches. The names of user interface elements are also bold, such as the names of dialog boxes and long program names.

Variables for which you must supply a value are in *italic*.

Code samples are in `monospaced` font.

Boxed Notes provide relevant information that is not directly part of the current thread.

Security Tip – Security tips and information related to the current thread.

Warning – Something to worry about concerning the current thread.

Note – Other information related to the current thread but that is not security related.

1 OVERVIEW

With more and more people working at home and connecting to company networks via the Internet, the risk to company networks to intrusion and theft of sensitive information is growing. Working from home has many positive advantages for both the home worker and the company they work for. However, as companies encourage people to work from home, they need to start considering the interaction of the employee's home network and the company network he connects to.

This paper discusses problems and solutions related to protection of home computers from attacks on those computers via the network connection. It does not consider protection of those systems from people who have physical access to the computers nor does it consider company laptops taken on-the-road.

Home networks are often targeted by intruders because they are plentiful and they are usually not well secured. While companies have departments of professionals to maintain and secure their networks, home networks are maintained by the employee who may be less knowledgeable about network security matters.

The biggest problems with home networks are that,

- Home networks are not designed to be secure and may use technologies (wireless) that are not secure
- The operating systems are not secured when they are installed
- The operating systems and applications are not maintained (for security considerations) after they are installed
- The networks are often used for other activities that put them at risk for being compromised

Home networks that are going to be connected to company networks need to be cooperatively secured by the employee and the company so they do not open up the company network to intruders. Securing home networks involves many of the same operations as securing a company network.

- Patch and maintain systems
- Securely configure systems
- Eliminate unneeded services
- Protect remote logins
- Use good passwords
- Use current antivirus software
- Moderate your Internet usage habits

Most of these items do not take a lot of work, but require an awareness of the risks involved in not doing them or doing them incorrectly.

The security of home networks and communications with company networks can be significantly improved by adding an appropriate software or hardware firewall to the home network and using a protected protocol such as Secure Sockets Layer (SSL), a

Virtual Private Network (VPN), or Secure Shell (SSH) for connecting to the company network.

2 INTRODUCTION

It was not that long ago that only a few people had home computers that they could use to dial into a work computer to transfer files, check running systems, monitor experiments, or administer networking. There was little risk to those systems as the connections between the two computers were direct, *point-to-point* connections through the telephone network. Because of this, no one worried that much about securing those systems.

That is not the situation today. Many people have a home computer that either belongs to their employer or that is their personal computer. They connect to a company *network* through the *Internet* in a variety of ways from *dial-up* connections to an *ISP*, to *broadband* connections through their cable TV, and to satellite connections. Many people have more than one computer at home, all participating in a home network. That home network is probably connected to the Internet, either intermittently through a telephone modem or full time through a broadband connection.

Note: Computer jargon terms shown in italics the first time they are used are defined in Appendix E – Glossary. More terms can be found online in The Jargon File (<http://www.tuxedo.org/~esr/jargon/>).

With all this connectivity, the home computer has become one of the primary communication mechanisms in the home. Kids use it to do homework and chat with their friends. Parents use it to communicate with friends, order from online catalogs, and do business correspondence. It may also be used to connect into the company network and do work via the Internet connection.

Along with all this computing and communications expansion, an increase in the number of intruders with accounts on the Internet has also grown significantly. In addition to the increase in numbers of intruders, their access to sophisticated intrusion tools has also grown with many “Hacker” websites devoted to teaching you how to break into a system and providing specialized *scripts* to automate the breakins.

Hackers are not the only security threat to home systems. Malicious code in all its forms (viruses, worms, Trojans) comes to you daily attached to e-mail messages and web pages. Or, is copied onto your system through open shares or through the use of system vulnerabilities. Malicious codes often open backdoors in systems for intruders to use.

Combining the growth of home systems, the growth in the numbers of hackers, the availability of hacker tools, and the growth of malicious code it is not difficult to conclude that home systems are vulnerable and likely to be attacked and compromised at any time. Except for when the home computer belongs to a company, it is the employee’s problem if his home network gets hacked. All of this changes, of course, when the employee uses his home computer or a company owned home computer to access company resources through the company firewall.

A company may have a good *firewall* maintained by knowledgeable administrators and have the internal network well patched and protected from intruders. The moment an

outside computer is allowed a connection to the internal company network it has potentially created a hole into that network. An intruder may then use that hole to explore and attack that internal network.

Security Tip: Portable systems that are used both at home and on a company's internal network can become Trojan horses that skirt the company's firewall and e-mail virus checking. These systems are considered "trusted" when they are connected to the internal network. If something made it onto the system while it was offsite, it can proceed to attack the internal network when the system is connected to the internal network. Users and management need to consider these risks as systems move between home and work.

PDA devices that are capable of file upload/download and e-mail also fit into this category and are proliferating widely.

This paper examines the threats to home computers and home networks via the network connection. It also examines the ways that you can protect an internal network from the mechanisms of intruders for different kinds of home networks.

- Single computer with a dial-up modem.
- Network with a dial-up modem.
- Single computer with a broadband connection.
- Network with a broadband connection.

This paper does not consider the security of systems related to people who have physical access to the system nor does it consider the security of company laptops taken on-the-road.

3 WHAT'S HAPPENING IN YOUR HOME COMPUTER?

Do you really know what is going on inside your home computer? Do you think it would be vulnerable to attack? Would you even know if it is or has been attacked? Without the right hardware, software, and security practices in place you won't have any idea what's happening in your system.

If you have a home computer that belongs to your company, you will have a user agreement that spells out if you can use the computer for personal as well as company projects. Most government owned systems may only be used for business related company projects. If your computer is limited to business related projects, it should only be used for such things as connecting to the company's internal network to transfer files or do other work. On the other hand, if it is your personal computer or you are allowed to use your company computer for personal projects, it is likely used for many other things besides connecting to the company network. You probably surf the Internet for information, or connect to catalogs to do online shopping. You probably read and send e-mail to friends and coworkers, and receive tons of spam mail.

If you have kids, they probably use it to do research for homework, search the web for information about the latest music, cloths, or other hobbies, and chat with their friends using e-mail and chat programs. They may have installed file sharing software like Kazaa or Morpheous to share music or other files.

If your computer were compromised by an intruder, virus, or worm, do you know what they could do to you or to others?

Some things they could do are,

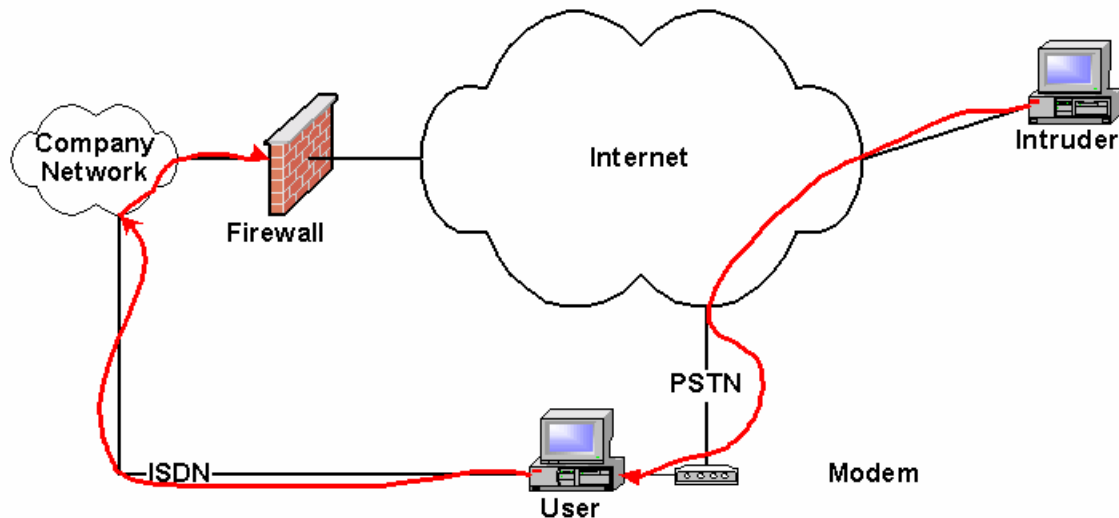
- Make you a conduit to the inside of the company firewall
- Use you as an attack site
- Spy on you
- Make you a DoS Drone
- Make you a worm breeding ground

All of these could have a significant impact on you, on your company, and on any sensitive information that you might deal with using your computer.

3.1 A CONDUIT TO THE INSIDE OF THE COMPANY FIREWALL

If we assume that you have a VPN or other connection to the inside of your company firewall, you could be providing a pipeline for an intruder to get in as well. If an intruder has broken into your machine and you are working on information through your connection to the company internal network, that intruder could be seeing the same information you are. The intruder could also be using your connection to connect to and download information from the internal network, install backdoor programs, and do other malicious things.

This scenario is not as far fetched as you might think. We have seen a system that had a telephone and modem connection to an ISP and a company owned ISDN connection to the inside company network. The user was surfing the web using the modem connection while monitoring processes on the company network. An intruder broke into the home system through the modem connection and attempted to transfer files between the internal network and an outside system. He was only discovered because his outbound connection did not go through the ISDN connection but through the company firewall which detected the connection and alerted security.



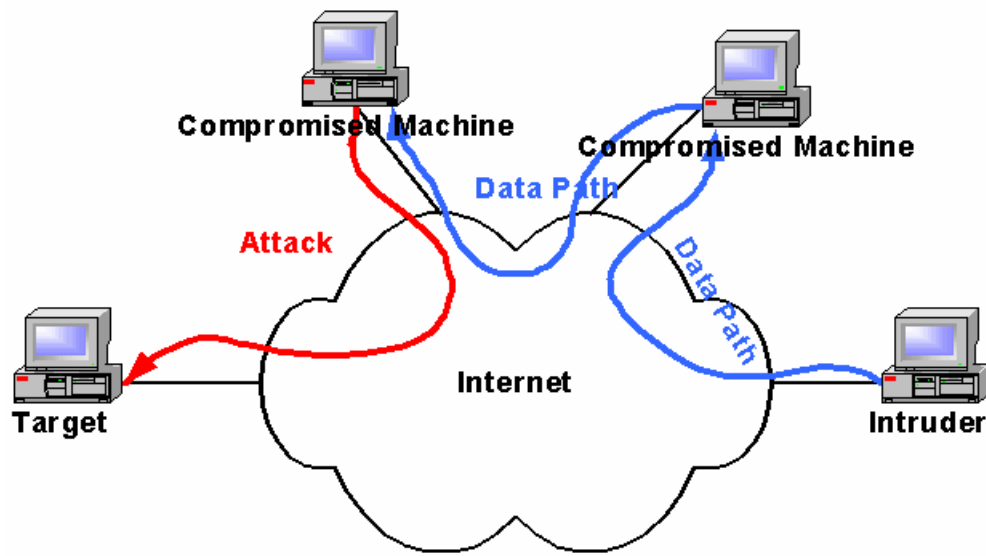
This type of breakin does not require two different network connections as in the example but could just as easily have been done through a single network connection to the Internet with a *VPN* connection to the company's internal network. A VPN connection makes the user's machine appear to be on the company's internal network by creating an encrypted pipe from the user's machine, through the Internet, to the company network. Packets destined for machines on the company network are directed through the VPN pipe. If *Split Tunneling* is enabled in the VPN, packets destined for the Internet go directly there and do not pass through the company network and the company firewall.

Security Tip: Split Tunneling is a configurable option on most VPN connections. If Split Tunneling is disabled all packets are sent through the VPN pipe so they have to go through the company network and out through the company firewall to get to the Internet. If Split Tunneling is enabled those packets destined for the Internet go directly to the Internet and only those packets destined for a company's internal network go through the tunnel. Forcing packets to go through the company firewall while an employee is working at home increases the load on the company firewall a small amount but lets the firewall help protect the employee's session.

Security Tip: You need to consider the security of a home system both while it is connected through a VPN to a company network and when it is not. A system that is protected only while it is connected to the company network can pick up a virus or worm and then pass that to the company network when connected through the VPN.

3.2 AN ATTACK SITE

One of the biggest uses for compromised machines is as platforms for attacking other machines. If the attack is detected, it can only be traced back to the last machine in the chain. To find the next machine you must get on the last machine and see where the packets are coming from that connect to it. You then go to that machine and find the next one down the line and so on. If the intruder stops his attack you cannot trace him any farther. Intruders often send their connections through a chain of several machines before attacking someone to hide their actual location from the authorities.



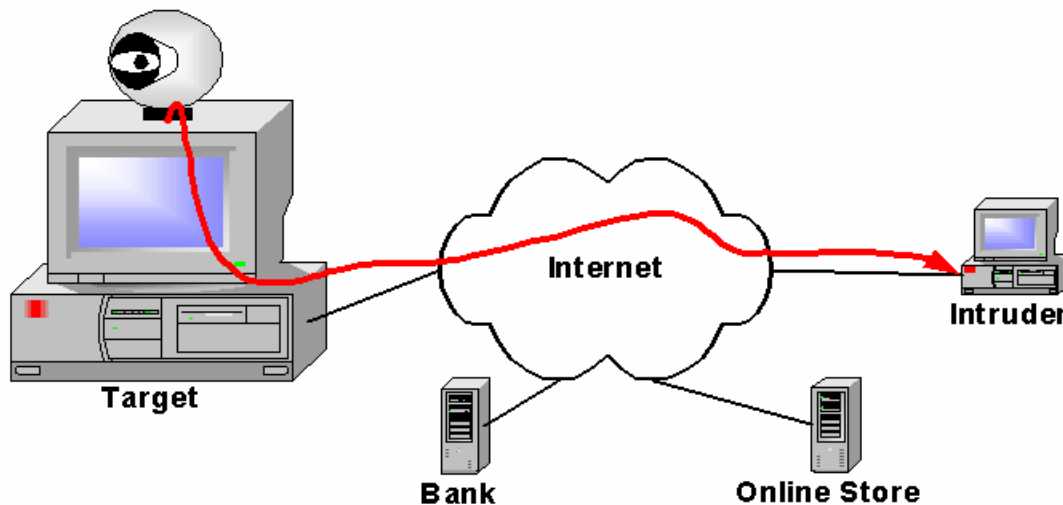
During the BIND/named attacks in 1998, hundreds of home computers were compromised and used to expand the attack. At the time, the new, broadband networks were populated with machines that had not been secured and thus were easy to compromise by the intruder.

3.3 A HOME SPY

Something most people do not consider is what an intruder could do to you if they have control of your computer. Basically, they can spy on you, see everything you do online and, in some cases, listen to or see into your home. For example, they can,

- Read all your documents.
- Change your documents.
- Read all your e-mail.

- Impersonate you while sending e-mail.
- Turn on a camera and watch you.
- Turn on a microphone and listen to you.
- Watch you login to network resources such as your bank or your company network.
- Capture everything you type at your keyboard.
- Delete things you want to keep.



We have seen backdoor programs (such as Back Orifice) installed on people's computers that give the intruder nearly full control of the computer. He can see an image of your screen, see where you click, and capture everything you type. If you happen to have a microphone or camera connected, he can turn these on and watch and listen to you as you work around your computer. If he chooses, he can move your mouse pointer and type on your keyboard to make it appear you are doing things that you did not do.

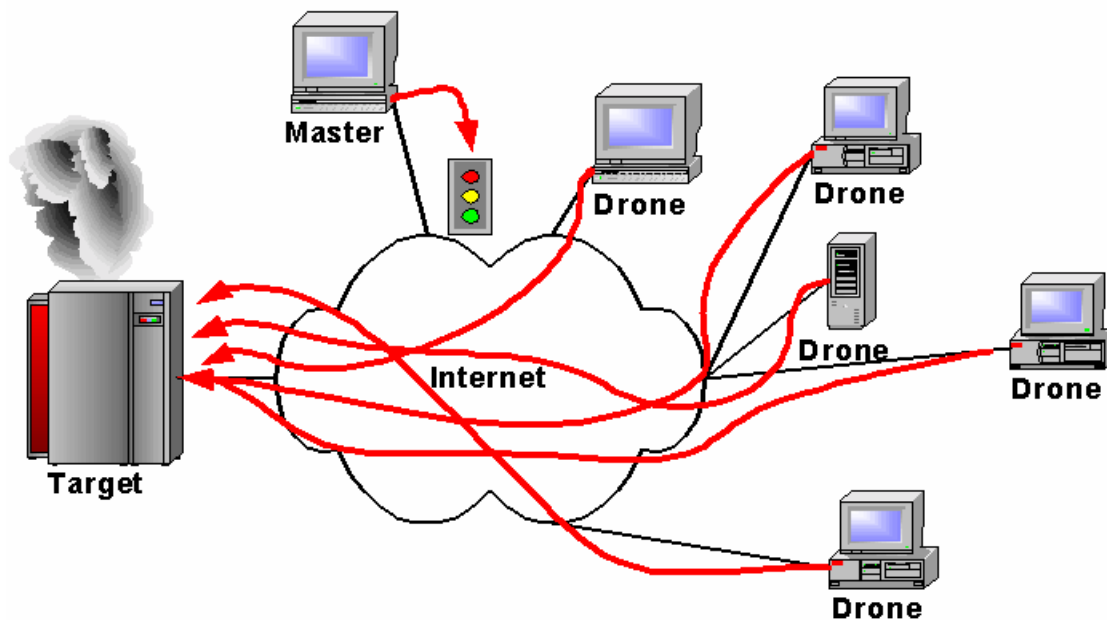
Back Orifice and other backdoor programs often come as attachments to e-mail messages that try to entice you to run them. Run them once and they disappear into your system where they are available for any intruder to come and use.

Security Tip: You can protect yourself from being observed or listened to by unplugging or turning off attached microphones and cameras. Keep in mind that most laptop computers come with a built-in microphone that cannot be unplugged. The only way to disable the microphone is to remove its software drivers. While those drivers could be put back by an intruder, it is unlikely he would have the correct drivers or that he would be able to correctly install them over a remote connection.

3.4 A DENIAL OF SERVICE DRONE (ZOMBIE)

An intruder planning a denial of service (*DoS*) attack needs to capture many machines to use as *DoS Drones* or *Zombies*. The *DoS* software is installed on these machines that then

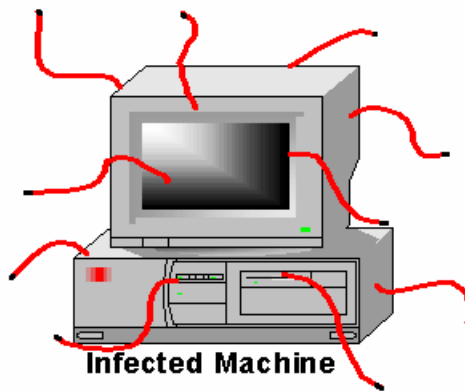
wait for commands from the DoS master machine. The commands tell the Drone what address to attack and what kind of packets to send to the attacked machine. Most often the packets are syn packets which tell a remote machine that you want to open a connection. If the attacker does not finish opening the connection, the half open connection sits there waiting until it times out. If you open enough half open connections in a short time, the server will not be able to open any new ones and legitimate connections will not be able to connect to the attacked machine.



This happened in 2000 when multiple home machines were used as Drones to attack Internet commerce sites.

3.5 A WORM BREEDING GROUND

Current malicious codes, known as *blended threats*, combine the characteristics of worms, viruses, and Trojans to attack systems. They are delivered to a machine by a web page, e-mail attachment, ICQ message or take advantage of a system vulnerability to copy themselves onto a target machine. When the worm code starts running on that machine, one of the first things it does is to create thousands of copies of itself and try to insert those copies in other machines.



Some real examples of this include: I Love You, Melissa, Nimda, MTX, FunLove, Hybris, Gibe, Glacier, Ramen, Code Red, Anna Kournikova, Sircam, Nimda ... Need I go on?

4 SECURITY RISKS OF HOME NETWORKS

Home networks are insecure from the start for several reasons.

- Operating systems are not secure
- Internet usage habits increase the risk of attack
- Internet connectivity increases the risk of attack
- Sharing systems among multiple users increases the risk of attack

Each of these problem areas needs to be considered and dealt with to harden a system from intrusion.

4.1 NEW SYSTEMS ARE NOT SECURE

Most new operating systems when installed out-of-the-box using the default installation settings are not secure. This problem has several causes, the first of which is that vulnerabilities have been found in systems after they were released to manufacturing. The intruders know about these vulnerabilities and, in many cases, have developed custom attack scripts to exploit them. While this may not appear to be a high risk for the short time it takes to patch and configure a system, we have seen systems compromised within hours of being attached to the network with a default system installation.

Many of the vulnerabilities in newly installed systems are as trivial as having a default password on the system that was not automatically changed during the installation process. Default accounts, blank passwords, and unprotected services make a system easier to install but their existence is well known by the intruder community. Problems like this should be fixed before attaching the system to the Internet.

The installation programs for many operating systems install everything possible during a default install. This is primarily a marketing ploy to make the system appear “Feature Rich”. Unfortunately, the more packages installed on a system, the higher the likelihood that one of them contains an exploitable vulnerability. This is especially true of network services, which open ports to the network. Every open port on a system is a doorway for an intruder to attack.

4.2 INTERNET USAGE HABITS

The second biggest increase in risk to home computers by hackers is caused by the huge changes in Internet usage habits that have occurred over the last few years. Previously, users would login, download e-mail or a single file, and then logoff. The amount of time a person spent connected to the network was minimal (you were being charged connect time by the minute) and the places he connected to were operated by known individuals or companies. With the advent of the World Wide Web and the commercialization of the Internet that has all changed.

There are now lots of things to do on the net. Browsing from website to website just to see what you can find (Web Surfing) is a hobby for many. People stay on the net for hours at a time, visit websites of unknown origin, go shopping at well known and

unknown online stores, and receive mail from all over the world. People visit websites containing any information that interests them, including those run by intruders.

Vulnerabilities in web browsers have allowed intruders to create malicious websites that attack users when they simply visit the website. While these vulnerabilities have been closed, we don't know when the next one will be discovered and put to use.

Another risk is that some people just can't resist pushing a button. Be it a button on a web page or an attachment to an e-mail message, if it is there, someone will click on it. The result is that one of the most common ways to get a virus, worm, or backdoor program run on a system is to simply e-mail the file to the owner of the system with a provocative title. Most intruders are not targeting specific systems so they send this infected message to hundreds of people and then check to see which systems are compromised. You can verify this fact by the large number of detected scans that are scanning for the ports of known backdoors. See Appendix D for a list of some of the known backdoor ports.

4.3 CHANGING INTERNET CONNECTIVITY

The risk to systems due to increasing Internet connectivity is significant. The primary reason for this increase is the amount of time a system is exposed to Internet attack. When the only way to connect to the network was a telephone and a modem, the window of opportunity for an intruder was only when the modem connection was open. With the availability of broadband connections including cable modems, DSL, and ISDN, that risk has increased. This is because most broadband connections are connected to the Internet all the time. If you leave your computer on all the time (as many do) it is exposed to potential attacks 24 hours a day as opposed to a few minutes a day for people who only dial in for email or two or three hours a day for people who spend a lot of time surfing the net.

Most intruders like finding systems with broadband connectivity because of its speed, reliability, and availability. If they are planning to use your system to scan networks or attack others, they need to be able to get in whenever they want and not just when you have dialed in with a modem. As we mentioned before, during the BIND/named attacks in 1998, hundreds of home computers on broadband networks were compromised and used to expand the attack. They were compromised because they were both vulnerable and accessible from the Internet.

Another, newer connectivity medium is Wireless. Wireless access points are often purchased, plugged in, and turned on. Most will work for you without any configuration. They also work for anyone else who happens to be in range (about half a city block for systems without any augmentation). Any intruder with a wireless card in range of your access point has full access to your subnet and gets to use your Internet connection for free. If you have a hardware firewall on your home network your wireless access point is likely behind that firewall which means the intruder is also behind your firewall.

4.4 SHARING SYSTEMS

Home systems are often shared by multiple people; spouses, children, room mates, and others. This sharing increases access to your files and increases the number of security mistakes that could be made in a system's configuration. While you may be careful what websites you visit and what buttons you push, others using your system may not be so careful and may cause the installation of viruses, worms, backdoors, and other malicious codes on your system.

As most home systems do not have the capability to segregate user access, anyone who can sit down at the system has access to all the files on the system and can install any software on the system. Systems of this type include: Windows 95, Windows 98, Windows ME, and Macintosh OS 9 and earlier.

Multi user systems that segregate user access and privileges significantly reduce this risk. These systems include: Windows NT, Windows 2000, Windows XP, Linux, and Macintosh OS X. These systems protect user files so that one user cannot access another user's files. User level privileges can be restricted so that normal users cannot modify system files and programs.

5 SECURING YOUR SYSTEMS

Securing your computer system starts the first day you turn it on. Your system should be updated and securely configured before connecting it to the Internet. If you must connect it to the Internet to download security patches, you should minimize the amount of time it is connected by disconnecting it as soon as the patches are downloaded.

Securing your system includes:

- Keeping the system software up-to-date
- Securely configuring the system
- Eliminating unneeded services
- Protecting remote logins
- Using good passwords
- Using current antivirus software
- Moderating your Internet usage habits

Most of these items involve some work when a system is newly installed or upgraded. After that, they generally need only be checked periodically to insure the system is still protected.

It is unlikely that these items will interfere with your “Internet experience” in any noticeable way. You will have to use good passwords to access Internet resources but it is not difficult to create passwords that are easy to remember and type. And, you will not be able to click on every button you see but the result is a much more secure system.

One more thing to note; your work computer is probably maintained by a security professional. Your home computer and possibly your work computer that you are using at home will have to be maintained by you. If you don’t think you can do this, you should find someone who can do it for you. It is not something you can ignore and hope it will go away because the hackers will find you if you don’t secure your system.

5.1 KEEP YOUR SYSTEMS UP-TO-DATE

The first step in protecting your system is to keep the system software up to date. This also includes any software that allows external connectivity to your system such as *web and ftp servers* and any *middleware* that is remotely executed via these servers.

Luckily, keeping your system up-to-date is becoming much easier as software manufacturers create automatic security notification and updating services. Much like antivirus updates, these services automatically apply security patches to your system software.

Security Tip: Software firewalls and other security software often replace system components with their own components in order to intercept malicious code and connections. Performing an update of operating system components may replace those components with updated system components, disabling the security software. You may need to reinstall such security software after updating your operating system. Refer to the manual for your security software to see if this is necessary.

5.1.1 Updating Windows Systems

Maintaining Windows systems has become much easier in the last few years because of the introduction of several networked technologies. First is the **Windows Update** web page (<http://windowsupdate.microsoft.com>). When you visit the **Windows Update** web page, a java script is run on your system that catalogs your current system state and compares that to a database. The comparison allows the program to determine what updates you have already installed and which ones you need to have a fully patched system. The web page then lists the patches you need and allows you to directly download and install them.

Complementing **Windows Update** is the **HFNetChk.exe** program available on the Microsoft website in the security tools area (<http://www.microsoft.com/technet/security/tools>). **HFNetChk.exe** works much like the **Windows Update** website in that it downloads a database file from the Microsoft website and uses that to determine what patches you have on your system and which you need to have a secure system. With **HFNetChk.exe** you can download the database file on one machine and copy it to another machine. In this way, you can check systems that are not connected to the Internet. Unlike **Windows Update**, after you have a list of needed updates, you must download and install the updates by hand. Note that **HFNetChk** works only on Windows NT/2000/XP systems.

Security Tip: New security patches are usually available to the **HFNetChk** tool before they are available from **Windows Update**.

The **Microsoft Baseline Security Analyzer** is a shell for **HFNetChk** that includes some additional checks of some critical security settings. It is also downloadable from the Microsoft website in the security tools area. The **Microsoft Baseline Security Analyzer** runs the **HFNetChk** tool and presents its results in a window with help and links to the patches identified by **HFNetChk**. In addition to scanning for needed patches, this tool also checks to see,

- That file systems are all NTFS
- If accounts have unexpiring passwords
- How many administrator accounts are on this machine
- If any accounts have weak passwords
- That the guest account is disabled
- That autologin is disabled
- That restrict anonymous is set as high as possible
- That Login success and failure is being audited

The program also lists some basic system information such as the number and name of shares, names of unnecessary services, checks for IIS and SQL server, and checks the Internet Explorer security zone settings. As with **HFNetChk**, this tool does not do the patching for you but this tool does have links to the patches to make them easier to find and download. The **Baseline Security Analyzer** also runs only on Windows NT/2000/XP systems.

The newest method of updating systems is with **Critical Update Notification** and its successor **Automatic Updates**. One of these two services is included with new versions of Windows. Older versions of Windows can download them from the Microsoft website. These programs query the Microsoft website in the background for new updates and security patches. Whenever one is found, they warn the user that an update is available and ask to install it. The user has only to authorize the update to have it automatically downloaded and installed on his system.

Security Tip: Windows 95 users will need to download and install any new security updates by hand as it is no longer a supported operating system. Older updates can still be installed with Windows Update.

The **Windows Update** and **Automatic Update** services are relatively up to date. However, to be as up to date as possible requires that you get a subscription to the Microsoft Security bulletins (<http://www.microsoft.com/technet/security/current.asp>). These bulletins will tell you about the latest security problems and allow you to download the individual patches before they are available on **Windows Update**. To update immediately or to wait for the patch to become available on the **Windows Update** or **Automatic Update** site depends on what is being patched and the severity of the patch. Generally, if the problem allows a *remote compromise* of a service that you are using, you should consider patching it immediately, otherwise, you can wait for the **Automatic Update**.

5.1.2 Updating Linux Systems

Maintaining Linux systems is much like maintaining Windows systems in that there is an automatic update service available for most versions of Linux. For example, Red Hat Linux has an update service that is part of the Red Hat Network (RHN). The **Red Hat Update Agent** can be configured to download all new updates and, if you choose, to automatically install them.

For versions of Linux without an update service, you need to subscribe to the security bulletins for your type of Linux. Whenever a security bulletin arrives, you need to determine the software that is being patched and the severity of the vulnerability. If you are using the software and the vulnerability allows a remote compromise of your system, you need to patch it immediately. If the vulnerability is less severe, you can wait and patch it when you have more time.

Patching Linux systems that don't have an automatic update service generally involves downloading the patch and running the patch installer. The installer takes care of

removing the older files and putting all the new files in the correct places. Installation instructions are generally included with or linked to by the security bulletin.

Security Tip: Don't install patches for services you are not using. Running the patch program will generally install the service. If the service is installed and you don't need it, simply uninstalling it removes the vulnerability.

5.1.3 Updating Macintosh Systems

Newer Macintosh systems (OS 9 and OS X) come with the **Software Update** service. This service automatically checks with the Apple website for software updates and warns you that the updates are available. You can then tell the service to download and install the patch.

You can get information about security updates on the Apple Security Updates web page (http://www.apple.com/support/security/security_updates.html) and by subscribing to the Apple Security-Announce mailing list (<http://lists.apple.com>).

5.2 SECURELY CONFIGURE YOUR SYSTEM

After a system is patched, it needs to be securely configured. Secure configuration consists of setting system options related to system and file access to values that reduce the risk of unauthorized access to that system or to its files. Most systems out-of-the-box are not secure even if they have all of the latest security patches. New systems almost always have default accounts, passwords, and settings that need to be changed before a system can be considered secure.

Warning: As with all things, be sure to backup our system before doing the configuration so you can get back to a working system in case you tighten things up too much.

Checking all these accounts and making all the appropriate security settings can be a difficult task, especially for someone who is not a knowledgeable system manager. This is especially true for the Windows NT/2000/XP systems that have hundreds of security settings. Luckily, there are tools available to help you find all the settings and set them to an appropriately secure value.

Warning: System configuration and hardening is not an exact science because of the many possible system configurations and applications that must run on those configurations. Be sure to keep track of the changes you make to a system because it is possible to lock down a system so tight that your applications will no longer. Using your notes, you can back out configuration settings in reverse order until you find the setting that makes things break.

This is also why it is a good idea to do the configuration after the operating system has been installed but before you have installed many applications. If you manage to harden a system so much that it no longer works it is not a lot of work to format the drive, reinstall the system, and start from scratch.

5.2.1 Securely Configuring Windows

Windows systems come in basically two flavors, the DOS shell systems (Windows 95/98/ME) and the NT based systems (Windows NT/2000/XP). While these systems look very similar at the desktop level, they are very different internally.

The Windows 95/98/ME systems are basically a Windows shell on top of a *DOS* system. The file system is one of the variants of the *FAT* file system and has no access protection built into it. These operating systems are basically for single user systems with little networked file sharing. They do not normally provide services to the network and hence have few holes for network attacks to use to break into a system. That said, if **File and Printer Sharing** is turned on and not secured or if **ftp** or **web servers** are installed and not secured, they can be compromised by an intruder. They are also vulnerable to the e-mail attachment worms and backdoors. After an intruder has compromised one of these systems, the intruder can do anything because there are no file access protections.

Logins to these systems are essentially unnecessary as hitting Cancel at the login prompt brings up a desktop. The username and password used at the login serve only to determine which profile to use when opening the desktop. Profiles contain information about what files are visible on the desktop, what programs are listed in the start menu, and what colors and pictures a user likes on his desktop. The profile also contains a list of accounts and passwords for networked resources that the owner of the profile likes to use. These accounts and passwords are stored in the profile to relieve the owner from having to type in a password every time he accesses a networked resource.

Security configuration of a Windows 95/98/ME system is minimal if file and printer sharing has not been enabled. Basically, if you do not provide any services to the network, it is impossible to compromise a system from the network. Keep in mind though that anyone who can sit down at the system has access to everything on it.

If file sharing is turned on, you must be sure to set security on the shared resources to block access to everyone who does not have a valid username and password. If you give everyone or guest access to your shared files and are connected to the Internet, then everyone on the Internet (anyone in the world) may share access to your files, not just those on your home network.

We recently helped a user recover some lost files on a system that was compromised by an intruder. The user purchased a new computer and put it on his home network. He then turned on file sharing with no passwords so he could copy files from his old computer to his new one. The user's network has a broadband connection to the Internet. An intruder started storing pornography on the user's system and when he ran out of space, he deleted a large folder. That folder just happened to contain the only electronic copy of the user's PhD thesis and all his research. Needless to say, he was not happy. Luckily, we were able to recover most of the lost files.

If you have added other servers to your system, such as **ftp** or a **web server**, be sure to configure these services to limit what an external user can do to your system. You need to be especially careful to limit an external user's ability to put files onto your system. If I can use **ftp** to put a file on your system in your web tree, I can put a Trojan or virus program there and get it executed on your system by simply selecting it with a web browser.

Windows NT/2000/XP systems are built on the NT technology which is a full preemptive multi-user operating system with file access protections built into the NTFS file system. The *NTFS* file system limits access to files to the owners of the files and to whomever the owners give permission to access. With the exception of the Administrator user, who has access to everything, normal users on an NT based system can only access those files they have been given permission to access. You must login with a username and password before you can have access to any files on the system. These systems also come with numerous network services installed by default that provide potential holes for an intruder to attack.

Securely configuring Windows NT/2000/XP systems is a lot more complicated than configuring Windows 95/98/ME systems. First, there are a lot more system settings that are related to system security. Second, each user has a separate account on the system and these accounts need to be configured to control what each user can do and what files the user can access.

The **Microsoft Baseline Security Analyzer** described in section 5.1.1 provides information on the critical things that need to be configured in Windows NT/2000/XP systems,

- Converting file systems to NTFS
- Set password expiration
- Test for weak passwords
- Disable the guest account
- Disable autologin
- Set Restrict Anonymous to a high level

File systems need to be set to NTFS for file access protections to work. FAT file systems have no access protections. The system needs to be set to force password changes in reasonable amounts of time and the Guest account must be disabled. **Autologin** causes a system to bypass the login process and startup directly with the primary user's desktop. Thus, anyone who can turn the machine on has the primary user's access. Restrict

Anonymous controls the amount of information that someone else can find out about your system over the network. It should be set to not give out any information to anyone who has not authenticated with the system.

If you have run the Microsoft Baseline Security Analyzer while patching your system you will already have information available about the most critical settings. In addition, Microsoft has made available security configuration checklists to help you make the security settings. These checklists are useful because they are not only a checklist, but have links to explanations about the settings and descriptions of how to make the settings. The checklists are available from the Microsoft website in the security area (<http://www.microsoft.com/technet/security>).

For Windows NT/2000/XP systems, the most critical setting is to insure that you are using the NTFS file system. Many NT systems are delivered installed on a FAT file system for ease of installation. If that is the case, you need to convert the file system to NTFS using the convert command. The convert command changes the file system to NTFS with all your files in place. That is, you don't have to save all your files and then restore them to convert a volume to NTFS. Open a command window and run the following command.

```
convert drive:
```

where *drive*: is the drive to convert.

Warning: You cannot convert a drive back to FAT after it has been converted to NTFS without reformatting the drive..

Most of the rest of the settings can be made with the **Security Configuration and Analysis Console** and the **Local Security Settings Console**. The **Local Security Settings Console** allows you to make most security settings one at a time. The **Security Configuration and Analysis Console** allows you to make Windows registry and other settings using a template instead of having to make each setting separately. Both Consoles are available in Windows 2000 and Windows XP, and are available as a downloads for Windows NT 4. The **Security Configuration and Analysis Console** includes a set of templates for different machines and for different levels of security.

The console file is **seconf.msc** and works with the **Microsoft Management Console** (MMC). The file is usually found in one of the two following directories,

```
%SystemRoot%\security  
%SystemRoot%\system32
```

where *%SystemRoot%* is the path to the Windows system directory (usually **C:\WINNT** or **C:\WINDOWS**).

The first set of templates are the default configuration templates and are found in the *%SystemRoot%\INF* directory. These templates define the default configuration of a newly installed Windows system. These templates can be used to restore a system to its initial security configuration.

deflwk.inf - Workstation
deflsv.inf - Stand alone server
defltdc.inf - Domain Controller

The security templates come in three different levels, basic, secure, and high-security, plus there are two special templates, dedicated domain controller and compatibility. Home users will likely only use the basic workstation or secure workstation templates. These templates are all in the default location for the **Security Configuration and Analysis Console**.

%SystemRoot%\security\templates

The basic security templates are primarily for reversing the application of the higher security templates. They set all the security settings to the Windows 2000 default values except for user rights.

basicwk.inf- Workstation
basicsv.inf - Stand alone server
basicdc.inf - Domain Controller

The Secure templates implement the recommended security settings for everything but files, folders, and registry keys. The default configuration for files, folders, and registry keys is considered to be secure.

securews.inf- Workstation or Server
securedc.inf - Domain Controller

The High-security templates add settings for secure Windows 2000 network communications to the Secure templates. These settings are only usable in a pure Windows 2000 network as older versions of Windows will not be able to communicate with this system.

hiseews.inf- Workstation or Server
hisecdc.inf - Domain Controller

The compatible template is primarily for upgrades of Windows 2000 from Windows NT. Windows 2000 Users have stricter security settings than Users in Windows NT so Windows 2000 Users may not be able to run some legacy applications that have not been certified to run under Windows 2000. The Windows 2000 Power Users are comparable to the Windows NT Users. If you do not want your normal users to be in the Power Users group in order to run legacy applications, you can apply the compatibility template which decreases the security of the Users group to the point where they should be able to run legacy applications.

compatws.inf- Compatible Workstation

Use the Dedicated Domain Controller template on domain controllers that do not run other server based applications. The security settings on Domain Controllers are designed to allow the Administrator run server based applications on the domain controller. This causes the security of the local Users group to be less than ideal. Apply this template on Domain Controllers that do not run other server based applications.

dedicadc.inf - Dedicated Domain Controller

A complete discussion of all the settings is beyond the scope of this report. Please see *CIAC-2321, Connecting to the Internet Securely; Windows 2000*, for a description of how to use the consoles and the contents of the templates for Windows 2000. For Windows NT and Windows XP the operation of the program is the same there are just more settings for Windows XP and fewer for Windows NT 4. Information is also available in the security area of the Microsoft website (<http://www.microsoft.com/technet/security>).

5.2.2 Securely Configuring Linux

As with Windows systems, securely configuring Linux systems involves many settings and adjustments. Couple this with the many different flavors of Linux and the number of possible settings becomes quite large. To make this a simpler task, there are a set of scripts known as Bastille-Linux which automate most of the security settings.

The scripts can be downloaded from: <http://bastille-linux.sourceforge.net>

Complete instructions for downloading and installing the scripts is available at that website.

5.2.3 Securely Configuring Macintosh

Macintosh systems come in two different flavors. OS 9 and earlier are the single user systems while OS X and later are the multi user BSD UNIX based systems. Like the Windows 95/98/ME systems, OS 9 has no desktop security. That is, anyone who can sit down at the computer has access to all the files on the system. From the network, there are almost no services available so there is almost no way for an intruder to get in. The one service that is available is file sharing. If you intend to use file sharing, be sure to create accounts with good passwords for the users you are going to allow to share files on your system and do not allow the Guest account to share files. Accounts are configured in the **Users & Groups** or **Multiple Users** control panels and file sharing is turned on or off in the **File Sharing** control panel. If you add any other network accessible services such as **ftp**, be sure to secure those services by disabling any guest accounts and putting good passwords on any user accounts.

Macintosh OS X has a core operating system based on BSD UNIX. After a system has been installed and patched, it is relatively secure from network attacks as it has few network services available in the default configuration. Turning on remote logins (**Sharing** control panel, Application tab, Allow remote login checkbox) starts an **ssh** server which is a secure login method. If you add other networked services, be sure to configure them securely.

5.3 ELIMINATE UNNEEDED SERVICES

Next, you need to eliminate all unneeded services. *Services* are programs that supply data or an action through a network *port*. For example, a web server is a service that supplies web pages through port 80 (and 443 if you are using SSL). If you are not using a service,

turn it off, or better yet, remove the service's software from your system. If the software is not there, you cannot accidentally turn it on.

Most home systems do not need any network accessible services. Home systems are users of services rather than providers of services. The services most often provided by home systems are file and printer sharing. These services should only be turned on if you need to share files and printers on your home network. If you have only a single computer on your network, you have no one to share with and should not install and enable these services. If you need these services, be sure to disable any guest accounts and use good passwords on those accounts that you do allow access.

When new systems are installed, the installers often install and enable every possible service. As mentioned before, they do this to make your system appear "feature rich" as a marketing ploy. It is also easier to install everything at once than to have to answer service phone calls from users who want to know why a feature does not work. However, every open service port is another target for an intruder to use to try to compromise your system. Even if the service is not itself vulnerable to attack, it may use other programs that are. For example, the Microsoft IIS web servers can be administered using **Microsoft FrontPage** and the **FrontPage Extensions**. If the access protections are set incorrectly on the **FrontPage Extensions**, an intruder anywhere in the world may edit your web pages.

If you later need a service you have removed, you need only reinstall it from the system installation CD. Don't forget to patch the newly installed service before turning it on.

A problem with many systems is you don't know what services are on and available over the network. Network scanners are very useful here to determine what ports are open on a system. Useful scanners include **nmap**, which runs on Windows and Linux platforms. Macintosh computers running OS X include a network scanner as part of the **Network Utility** program.

5.3.1 Windows

Services are removed from Windows systems by either uninstalling them with the **Add/Remove Programs** control panel, by turning them off with a control panel or registry setting, or by disabling them with the **Services** control panel. For example, the IIS server includes a web server, ftp server, gopher server, index server, mail server, and news server. Using the **IIS Setup** program or the **Add/Remove Programs** control panel you can add or remove any of these services. You can turn individual services on and off without removing them using the **Internet Service Manager** snapin to the **Microsoft Management Console**.

Other services may not be so easy to turn off. For example, Novell networking can only be turned off by uninstalling the network driver.

The **srvinfo.exe** program included in the Windows NT Resource kit gives you a list of running services on Windows NT, 2000, and XP computers but it is difficult to tell from

the list which services are accessible through the network. The **Service Installation Wizard (srvinstw.exe)** is also useful for determining which services are active and for turning them on and off. Again, it is difficult to tell from the services list what services are actually accessible from the outside.

Windows NT and newer systems contain the **netstat.exe** program that is similar to the UNIX **netstat** program. Running the command **netstat -a** gives a list of all open ports on a system. Keep in mind that some network ports are actually used for interprocess communications within a system and are not really accessible on the external network.

File sharing on Windows systems is enabled with a check box on the networking control panel. The path to this control depends on which version of Windows you are using. In Windows 2000, select the **Network and Dialup Connections** control panel and open the properties of the **Local Network** connection. Uncheck **File and Printer Sharing for Microsoft Networks** to disable sharing or click Uninstall to completely remove that capability.

Another option is to control access to the network ports. In this way, if a port happens to be open, you can block access to it. Beware though that you don't block a needed port. Windows XP has a built-in software firewall (discussed later) that you can use to block access to ports. In other versions of Windows you need to use **TCP/IP Filtering**. To turn on this feature, you need to get to the properties of the **Internet Protocol (TCP/IP)** control. The path to this control depends on the version of Windows that you are using. In Windows 2000, you select the **Network and Dialup Connections** control panel and open the properties of the **Local Network** connection. Find the **Internet Protocol** and select properties again. In the Internet Protocol properties click Advanced, and then the Options tab. In the Options window select **TCP/IP Filtering** and click Properties. The open dialog box allows you to specify which ports can be connected to on your system and block access to all others. Be careful that you do not block ports and protocols that you need.

5.3.2 Linux

Services in Linux and other UNIX systems are turned on and off in one of several ways depending on the particular system. If you are using one of the configuration tools, such as Bastille (discussed previously), you can use the tool to turn things on and off. Otherwise, you will need to do it manually.

The most common places are in **/etc/inetd.conf**, in the **/etc/rc1.d**, **/etc/rc2.d**, etc. directories, and in the startup scripts. If **inetd** is running, the most common network services are started there. Services available through the **inetd** service are turned on and off by simply commenting them out of the **/etc/inetd.conf** file and sending the HUP signal to **inetd**. First, open **inetd.conf** with a text editor and find the line that starts the name of the service you want to stop. The line begins with the service name such as **ftp** or **telnet**. Insert a pound sign (#) as the first character in the line for the service you want to disable and save the file. Next you need to send **inetd** the HUP signal. First, run the **ps**

command and find the process number (pid) for **inetd**. To send the HUP signal, issue the command,

```
kill -HUP pid
```

Services that need to be running all the time are either started from within one of the startup scripts or by placing a link to the startup script for the service in one of the **rc*.d** directories. If the service is started in one of the startup scripts, locate it by grepping for the executable file name in the **/etc** directory. If the service is started in one of the **rc*.d** directories you locate it by first locating the startup file in the **/etc/init.d** directory. Next look in the **/etc/rc2.d** and **/etc/rc5.d** directories for a link to that file that starts with an S. The **rc2.d** directory contains the startup commands for the programs that run in *runlevel* – 2 which is the normal multi-user runlevel in Linux with a command shell interface. The **rc5.d** directory contains services to startup a system in a multi-user mode with a *gui* interface. Removing that link disables the service. Many flavors of Linux come with a *gui* runlevel editor. Using this editor you can easily turn services on and off for different runlevels.

Some newer versions of **Linux** use **Service Configuration (serviceconf)** *gui* program to turn services on and off. If that program is used to configure your system, you must use it to turn things on and off.

To completely remove a service, delete the executable files from the system that start the service *daemon*. Most common services are in **/usr/sbin** and have names that start with “in.” and end with “d”. For example, the ftp service is named **in.ftpd**. If you remove this file from your system and do not remove the startup script, you will see the startup script complain at system boot time but the system should still boot.

In systems that use a package manager like **rpm**, the manager should be used to remove the service executable files instead of deleting them by hand. The package manager knows where all the parts of the service are and can remove them all.

You can determine which ports are actually open on a Linux system by scanning or using the **netstat -a** command. The **netstat -a** command lists all open ports. You need to be careful as not all open ports are actually accessible from the external network. This is because UNIX systems often use network connections for process communications even though the two processes are on the same system. Connections and open ports marked as **localhost.nnn** where *nnn* is the port number or *machinename.nnnn* where *machinename* is the name of the computer are connections between processes on the system.

This confusion about internal and externally accessible ports is why port scanning is useful for unambiguously determining which ports are really open.

Another service configuration for Linux is to install **TCP Wrappers**. **TCP Wrappers** is a filter for services started in **inetd.conf** that limits what addresses external connections can come from. If you must use an insecure service such as **telnet** or **ftp**, **TCP Wrappers** are essential to control which external machines are allowed to connect to that service. Without **TCP Wrappers**, anybody on the Internet can try to connect to your service.

TCP Wrappers is included with most versions of Linux and just needs to be installed. If wrappers is not included, it is available from,

<http://www.porcupine.org>

After installation, place service names and address ranges that are allowed to connect to the service in the **/etc/hosts.allow** file. See the man pages for the file format.

Security Tip: The **ssh** server also uses the **/etc/hosts.allow** file to control where **ssh** users can connect from even though it is not normally started with **inetd**. To do this, **sshd** must include the wrappers library when it is compiled.

The Bastille program mentioned in the earlier section on securely configuring Linux can aid you in disabling unneeded services.

5.3.3 Macintosh

A Macintosh running OS 9 and earlier has all of its services controlled with a control panel. OS 9 has few network services to begin with unless you have added services from third parties such as an ftp server. Generally, the service can be turned on and off with the control panel and the software can be removed using the **Extensions Manager** control panel to remove the control panel or extension that maintains the service. Also with the **Extensions Manager** control panel, you can move the service back if you need it.

Security Tip: The **Extensions Manager** control panel does not remove software from the system, it just moves that software to a different folder. For example, disabled extensions are moved from the Extensions folder to the Disabled Extensions folder.

A Macintosh system running OS X is just a BSD UNIX system with a Macintosh shell running over it. Most of the common services are turned on and off using **System Preferences**. For example, the **Sharing** control panel in **System Preferences** turns **ftp**, **www**, and **ssh** services on and off. Making changes in the control panel actually makes changes in the text file **/etc/hostconfig** which is used to determine what services are started on a system.

Security Tip: The **Sharing** control panel is a little cryptic about what services are being turned on and off. For example, the **Allow Remote Login** check box turns on the **ssh** protocol.

Most of the executables that are started up in a system are stored in the **/System/Library/StartupItems** directory in subdirectories that have the services name. At boot time, the system tries to start all services in that directory. Some may not start because of settings in the **/etc/hostconfig** file but others must be removed from the **StartupItems** directory to turn them off.

Another option in OS X is to use the built-in software firewall **fwvm**. This firewall is a simple packet filter and cannot do *stateful* analysis.

Some options are:

- ipfw list** -- list the current rule set.
- ipfw show** -- list the rule set and the counters associated with the rules.
- ipfw flush** -- delete all but the last rule.
- ipfw delete** *number* -- delete a rule.
- ipfw add** *rule* -- add a rule.

A rule is created in the following form,

[*number*] action [log] proto from src to dst [via name | ipno] [options]

where *number* is an integer between 1 and 65534 which determines the location of the rule in the rule set. Rules are tested from the top down and the first rule to hit is executed. Rules without a number are added to the bottom of the list above the last rule. Since **ipfw** runs in a default system the last rule is usually,

allow ip from any to any

action = **allow, deny**

proto = **udp, tcp, icmp**

src, dst = source and destination addresses and optional port numbers.
address/mask [ports]

For example: 192.168.5.1/24 for all addresses on the 192.168.5.x subnet.

name = The name of the interface (en0).

ipno = The ip address associated with the interface.

options = **in** -- incoming packet, **out** -- outgoing packet,
setup -- open connection packet.

As mentioned above, OS X comes with a port scanner in the **Network Utility**. Use this scanner to determine which ports are open. You can identify which service uses a port by looking in the **/etc/services** file. As OS X is UINX based, you can open a terminal window and execute the **netstat -a** command to display all open network ports. As with Linux, many of the open network connections are not open to the outside but are only open to internal services as network connections are often used for processes to communicate with each other.

In the sample output below, the ports whose local address starts with **localhost** are not accessible externally. There are three open tcp ports in the example: **ssh, ftp**, and 3639. On the udp side, ports 137, 138, 855, 2222, **syslog**, and 49156 are open. Ports with names defined in the **/etc/services** file are listed with their name instead of a port number.

```
root# netstat -a
```

Active Internet connections (including servers)

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	(state)
tcp	0	0	localhost.1033	localhost.887	ESTABLISHED
tcp	0	0	localhost.887	localhost.1033	ESTABLISHED
tcp	0	0	*.ssh	*.*	LISTEN
tcp	0	0	*.ftp	*.*	LISTEN
tcp	0	0	*.3639	*.*	LISTEN
tcp	0	0	localhost.815	localhost.1033	ESTABLISHED
tcp	0	0	localhost.1033	*.*	LISTEN
udp	0	0	*.2222	*.*	
udp	0	0	*.138	*.*	
udp	0	0	*.137	*.*	
udp	0	0	*.49156	*.*	
udp	0	0	localhost.49155	localhost.855	
udp	0	0	localhost.49154	localhost.855	
udp	0	0	*.855	*.*	
udp	0	0	localhost.1033	*.*	
udp	0	0	*.syslog	*.*	
.					
.					
.					

5.4 USE REMOTE SERVICES THAT PROTECT THE LOGIN

Older network communications services pass a password in the clear over the network that any listening machine can capture. Programs like: **ftp**, **telnet**, **rsh**, and **rlogin** all pass their passwords in the clear. This is a security problem because **sniffer** programs are readily available for most operating systems and can capture the packet traffic on the networks they are connected to. If your connection to a server passes over the network where a **sniffer** is listening, the **sniffer** can get your login name and password.

Use instead services that use encryption or a challenge-response (one-time password) method of authenticating. For example, the following services protect their logins and, in some cases, protect the whole communication stream.

Opie (s-key), SSH, VPN, NTLM, NTLM2, AppleShare

Opie is a new version of the **s-key** program that generates one-time passwords for logins to systems. You can either generate a list of passwords that each works once or you can use the **Opie Calculator** that combines a challenge with a user's pin to calculate the one-time password.

Ssh (Secure Shell) is available for most operating systems in both commercial (F-Secure SSH) and public license versions (OpenSSH). **Ssh** is a good replacement for **telnet**, **ftp**, **rlogin**, **rcp**, **rsh** and others. **Ssh** uses public key cryptography to create an encrypted link between two systems. Passwords are then exchanged within the encrypted link.

VPN comes in many different forms and is a way for creating an encrypted pipe between two systems or a system and a network. All communications between the systems go through the pipe and are protected.

NTLM, **NTLM2**, and **AppleShare** are all network file sharing systems that use challenge response methods of authentication.

Security Tip: don't forget to keep your secure communication software up-to-date.

5.5 USE GOOD PASSWORDS

Passwords are the primary method of authentication used for most systems, especially home systems that cannot afford the expense of key cards and other more exotic authentication methods. However, do you really know what the login password does? Keep in mind what the password really protects when logging into a system.

On Windows 95, 98, and ME the login password unlocks the password file which contains the passwords needed to connect to networked resources. It does not control access to any files on the local machine. You can easily login to the local machine with no password by simply clicking cancel at the login. This password protects access to remote resources only.

On Windows NT, 2K, XP, Macintosh OS X, LINUX and other UNIX like operating systems, the login password controls access to the local files on your system as well as to remote resources. On these systems, the login password does what you would normally think a password does.

Security Tip: Keep in mind that if someone has physical access to a system there are ways to get access to the contents of the hard disk without needing a password. The only protection against this type of access is an encrypting file system.

On Macintosh OS 9 and earlier systems there is no login password required. OS 9 and earlier systems do have a password keychain for storing network passwords. The keychain is an encrypting security container for passwords and is not unlocked at login time but remains locked until one of its passwords is needed. You then must type in the master password to unlock the keychain.

5.5.1 Choosing Password Complexity

It used to be that a password just had to be hard for a person to guess. Now, sophisticated *password cracking programs* are used to guess and crack passwords. These cracking programs use whole dictionaries of words to crack a password. If a password is in a dictionary, including foreign language dictionaries, it can be cracked relatively easily. Modern cracking software also knows about words plus numbers or words plus letters so a word with a number or letter added to the beginning or end is also crackable. Using a good password requires that you make it difficult for a machine to guess which means forcing the cracking program to have to try all possible letter, number, and symbol combination to get it.

Security Tip: If a password cracking program has a copy of your encrypted password, it will eventually crack it. The trick is to make it take so long to crack that the hacker using the program gives up.

Security Tip: Password cracking programs need a copy of the encrypted password to work. They then test possible passwords by encrypting them and comparing that to the encrypted password. Without that, they must attempt to login to a system to test a password which takes much longer to do. Protecting access to the encrypted passwords makes a system much more difficult to break into.

Security Tip: Password cracking that involves logins to a system to test the passwords can be thwarted by setting the system to disable an account after a small number of failures (say 5). The account can be set to be automatically reenabled after 30 minutes but that wait makes the password cracking take years. On Windows systems, network logins to the Administrator's account can also be set to lock out after some number of failures even though the console login to the Administrator's account cannot.

Security Tip: Windows systems send the encrypted password over the network for network logins. To be able to login to legacy systems that use the LanMan protocol (Windows 3.1, 95, 98), a simpler encryption of the password is also sent to the system being logged into. This simply encrypted password can be captured and cracked by any system connected to the network. Unless you absolutely must allow LanMan logins, they should be disabled on all Windows systems and instead use NTLM or later.

Security Tip: On Windows systems, run SysKey, which increases the level of encryption for keys stored on the system, eliminating some of the LanMan vulnerabilities for the stored keys. This does not protect LanMan keys sent over the network during a login. Syskey is available on current versions of Windows and is downloadable from the Microsoft website.

To make the password unguessable, it should not be any variant of the machine name, the user's name, or the user's account name. Variants include writing the word forwards, backwards, with mixtures of upper and lower case, with another character added to the beginning or end, or any combination of these.

To make a password that is not susceptible to a dictionary attack, it should not consist of a dictionary word, a backwards dictionary word, or a dictionary word with a character added to the beginning or end. As password cracking programs can also use foreign dictionaries, foreign words should also be avoided.

Create a good password by maximizing the "key space" that must be used to find the password. Most password cracking programs try simple key spaces first. For example, the lower case alphabet. If a password is not found in a simple key space, the cracking program must resort to larger key spaces. Create a good password by using characters from at least three of the following key spaces.

- lower case letters
- upper case letters
- numbers

- symbols

Security Tip: To make passwords easier to remember, come up with an algorithm that is easy to remember. For example, choose a sentence and use the first character or last character of each word (such as, My Bonnie lies over the ocean = MBloto). Or, two words interspersed within each other (such as, key + space = ksepyace). Add some capitals and numbers or symbols and you have a good password.

5.5.2 Choosing Password Length

The length of a password is also a concern. Shorter passwords are easier to guess but longer passwords can be difficult to remember. Each character you add to a password increases the number of possible combinations by a factor of 94 (= 26 lower case + 26 upper case + 10 numbers + 32 symbols). Six characters should be considered an absolute minimum for a password with eight being the current standard.

Security Tip: Windows systems that must allow LanMan logins (that is, they cannot upgrade to NTLM only) should be a minimum of 7 characters. Increasing this to 8 or 9 characters does not improve the security. This is because the LanMan password is actually stored as two 7 character passwords with each encrypted separately. While a 10 character password might seem to be much stronger than a 7 character password, it is actually stored as a 7 character password plus a 3 character password. Cracking the 3 character password is trivial for most password cracking programs. Security isn't really improved until you use a 14 character password and even then it is only minimally improved.

Improving the security of 7 character LanMan passwords can only be achieved by widening the keyspace through the use of symbols as shown in the last section.

5.5.3 Protecting the Encrypted Password

You would think that the encrypted password would be protected by default on most systems. However, that is not the case because of the need to connect to legacy systems. UNIX type operating systems (Linux, Solaris, etc.) originally placed the password in the /etc/passwd file (a logical place) however they also put other information, such as the location of the user's home directory, in the same file. That other information was needed by other applications so the password file was readable by anyone. As such, it quickly became a target for intruders. Newer versions of UNIX have moved the password to the /etc/shadow file that can only be read by the root user.

Windows systems use a multitude of network authentication methods, including the older LanMan authentication. LanMan authentication actually splits the 14 character password into two 7 character upper case passwords. It then sends sufficient information over the network during authentication to retrieve the encrypted password. The fact that it consists of only upper case letters and that it can be treated as two 7 character passwords makes it relatively easy to crack. If at all possible, you must disable LanMan authentication and use only NTLM or later authentication on PC systems. You should also install SysKey to

better protect the stored copies of the password. SysKey reencrypts the hashed 14 character password with a 128 bit key to make it almost impossible to crack. Keep in mind though that SysKey only protects the copy of the encrypted password when it is stored on your computer. It does not protect the copy that is sent over the network during a login.

Security Tip: If you disable file and printer sharing the only keys you must protect are the ones stored on disk. Protect the ones on disk with SysKey.

Warning: Be careful when you use SysKey. Save a backup copy of your unencrypted registry before installing SysKey so you can restore things if they go wrong.

LanMan authentication cannot be disabled on Windows 95/98 without disabling all file sharing. LanMan authentication is disabled on Windows NT/2000/XP with a registry setting which can be made with the **Security Configuration and Analysis** tool which was discussed earlier.

In a home network consisting of a single machine in most cases there is no reason to have file and printer sharing turned on. If you turn file and printer sharing off, you won't have the problem of network passwords going out over the Internet. If you do need to share files with a remote system on the Internet you should find a safer way to do it other than Windows file sharing. For example, use a firewall and a VPN connection to the remote system.

In a small, home network consisting of more than one computer, you may need to share files among the computers on that home network. Keep in mind that when you are turning on File and Printer sharing that you are sharing with the whole Internet. In this case, you need a firewall between your home network and the Internet to keep the sharing within your home network. Sharing of files within a small home network, even using LanMan authentication is not a high risk as only users on the home network would be able to capture the encrypted passwords. Again, if you need to share files with a system across the Internet you should use a protected connection such as VPN.

5.5.4 Determining When to Change Passwords

There is a lot of controversy about changing passwords, when you should always change them, when you should routinely change them, and the risks of not changing them. Passwords should be changed immediately if one of the following conditions occurs,

- An intruder has captured your encrypted password.
- You believe someone was shoulder surfing and saw you type your password.
- A laptop with your saved network passwords has been stolen.
- A system with your password on it has been compromised.
- A sniffer was found running on your subnet.
- You suspect your password may have been compromised.

All of these basically say that if you think your password has been compromised in any way you need to change it immediately. This is not a “Do it when I get around to it” activity. If an intruder has your password, he will likely use it within a few hours or less of obtaining it. Putting off the password change until tomorrow may be too late.

When should you routinely change your password, or, more importantly, why should you routinely change your password? Changing your password every *nn* days has been a computer maxim dating back to the beginning of time sharing systems. Most people never question it and dutifully change their passwords when required to do so. But, why should you do so at all?

Password changing became a requirement when users started connecting to network resources using passwords sent in the clear over the network. Passwords sent in the clear over a network have the vulnerability that anyone with a machine on that network can listen to the packet traffic and capture a copy of your password. Intruders built special sniffer programs that automatically capture the first *n* bytes (usually 128) of each *login session*. The first 128 bytes almost always contains the username and password used to open the session.

Security Tip: The replacement of network hubs with network switches has all but eliminated the usefulness of these sniffer programs. With switches in place you can no longer sniff all packet traffic on a network. You can only sniff traffic to and from the machine the sniffer is running on. On the other hand, a sniffer running on a server can see all logins to the server even though the server is connected through a switch.

Passwords should be routinely changed in the amount of time that it would take an intruder to get your password, crack it, and use it to break into your system. Routine password changing times range from 15 days to never with about 180 days being the current standard. But, why change your password at all? If an intruder has your password, they are probably going to use it in less than a day so you should be changing your password daily. If an intruder does not have your password, he cannot use it to break into your system so you do not need to ever change your password.

Before determining how often you should change your password you need to consider the following items.

- Does an intruder think you are a target?
- What could an intruder do if he did break into your system?
- How badly do you want to keep an intruder out of your system?

The first item does not concern what you think, it is concerned with what an intruder would think. If you have any computing power of any kind the intruders want you so the answer to this question is likely always yes.

Most intruders are looking for systems to use to attack others and you don’t want to be the source of attacks on other people’s systems. So, the answer to the second item is, “Lots of bad things.”

Unless you don't use your system for anything, you likely have personal data on it. E-mail, personal letters, business letters, research reports, and other information that you would likely prefer that an intruder stay out of. There is likely enough information on your system for an intruder to commit identity theft and you really don't want that to happen.

Now that we have settled the fact that you are a target and you really want to keep an intruder out of your system, how often should you change your password? If an intruder can get a copy of your encrypted password, how long will it take him to break it by trying every possible combination of numbers, letters, and symbols?

To get a feel for how quickly passwords can be cracked, the L0phtCrack password cracker was tested on a 150 MHz Pentium system cracking 14 character random passwords made up of a mixture of upper and lower case letters and numbers. It was able to crack 3 such passwords in 24 hours. L0phtCrack attacks the 14 character LanMan passwords which are actually two 7 character passwords with all characters shifted to upper case, this amounts to cracking six 7 character passwords in 24 hours or about 3 hours per password (Randy Smith, "Protect Your Passwords," *Windows NT Magazine*, Oct., 1998, p. 127).

As these passwords are random, a dictionary attack will fail and a brute force attack must be used. For 7 character passwords utilizing upper case letters and numbers, there are $(26 + 10)^7 = 36^7 = 7.8 \times 10^{10}$ possible passwords to try. On the average, you should find a password by trying only half that many passwords.

If LanMan is disabled and NTLM is used, the full length of passwords becomes important and not just the first 7 characters. In this case, assuming you are using a wide keyspace as described in the last section each additional character multiplies the time needed to crack a password by a factor of roughly 100 (26 lower case + 26 upper case + 36 symbols + 10 numeric digits) = 98. If a 7 character password can be cracked in 3 hours an 8 character one would need 800 hours or about 30 days.

Unfortunately for security, computer processors have gotten much faster since 1998 with top speeds around 3 GHz. If password cracking scales with processor speed, the 800 hours would be reduced to 40 hours for an 8 character password or 163 days for a 9 character one.

Based on this data, you should disable LanMan authentication or at least not allow its unencrypted use over the Internet, use 9 character or longer passwords, and change them about every 6 months just in case someone has managed to get a copy of the encrypted password. If you allow unencrypted LanMan authentication over the Internet or other public networks you should change your password more often.

Security Tip: Because of the speed with which systems are getting faster, most security shells and programs no longer ask you for a password, they ask for a pass phrase, indicating that they want something more like a short sentence than a single word. This is to get you prepared for the time when 7 or even 14 characters is too short of a password. If you use a short sentence as a pass phrase leave out the spaces. Leaving out the spaces prevents the cracking program from using statistical analysis to speed its chances of finding a match. Other options to increase the security but still have an easy to remember pass phrase are to use other characters in the spaces and to misspell words.

5.6 USE CURRENT ANTIVIRUS

The huge growth in network aware viruses and worms makes it imperative that you use current antivirus software with automatic updating and realtime protection. New viruses and worms appear on a daily basis so you must have an up-to-date antivirus scanner in order to detect them. You must also have realtime protection enabled to catch viruses and worms as they enter your system and not depend on a virus scanner to catch them at a weekly scan.

We cannot emphasize enough the need for an up-to-date antivirus scanner. By up-to-date, we mean one that has virus definitions that are no more than a week old. Modern viruses have a window of opportunity of no more than a day or two to infect as many machines as possible before the antivirus vendors have a detection string available. If you do not have current antivirus on your system, or have not updated it in a while, you have expanded that window of opportunity to weeks or months.

Consider, for example, the Klez worm. We currently see about fifty infected messages a day sent to one public e-mail address. And, this is after the signature for Klez has been available for several months. This indicates that there are a lot of people out there with unprotected machines that have the Klez infection.

To keep a system up-to-date you need a scanner and a subscription to an update service. Current update services are around \$10 per year, which is well worth the increased security. With a current scanner, you will be at risk to a new virus or worm for no more than a couple of days.

The second thing you must have is realtime protection. Realtime protection scans all new files as they are placed on a system and all e-mails as they are sent or received. With an up-to-date scanner, you will likely capture any virus before it gets on your system. With a good, realtime scanner, you should not need to perform regular scans of your system as all new files are checked before they get on your system. Weekly scanning is useful to catch those few new viruses that might have gotten on your system in the virus window of opportunity.

Security Tip: Keep in mind that most modern viruses and worms actively search for antivirus programs on disk and in memory and disable them. If a virus has both gotten on your system and gotten executed, it may be impossible to detect and remove it using a routine, weekly scan. If you suspect you have a virus infection, you need to boot your system using a known clean (uninfected) disk before doing the scanning.

5.7 MODERATE YOUR INTERNET USAGE HABITS

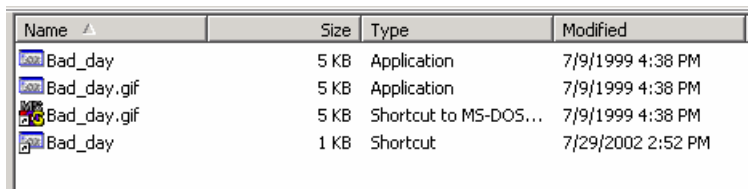
This one comes under the topic of self discipline during Internet usage. Poor habits when visiting web pages or reading e-mail are the source of many security problems. Some things to keep in mind are,

- Don't double click on any attachment to an e-mail that you are not sure of.
- Be careful what you download.
- Don't visit dubious websites without having the security settings of your web browser locked down to prevent scripts from running.
- Don't give out login information to dubious websites.
- Don't give out personal information to dubious websites.
- Ignore Internet rumors.
- Turn off systems that are not in use.

Attachments to e-mail messages can have their extensions hidden to make them appear to not be an executable file when they actually are. If you have "Hide extensions of known file types" turned on in an **Explorer** window, you will not see extensions like **.com** and **.exe**. Malicious code files are often named things like **mypictures.gif.exe**. If you have the extensions hidden, you will see **mypictures.gif** in a file listing, which appears to be a picture file. In actuality, it is an executable. Make sure extensions are not hidden.

Even with extensions not hidden, there are executable file extensions that are always hidden. For example, **.pif** (dos executable setup file) is an executable extension that is always hidden as is **.lnk** (shortcut).

For example, take a look at the following image of a **Windows Explorer** window. These are three copies of an executable file and a link to that executable. All are executable.



Name	Size	Type	Modified
Bad_day	5 KB	Application	7/9/1999 4:38 PM
Bad_day.gif	5 KB	Application	7/9/1999 4:38 PM
Bad_day.gif	5 KB	Shortcut to MS-DOS...	7/9/1999 4:38 PM
Bad_day	1 KB	Shortcut	7/29/2002 2:52 PM

Below is a listing in a **Command Window** of the same directory in the same order as the **Windows Explorer** window. In the **Explorer** window the first two files are **.exe** files even though the second has the **.gif** image file extension. In the **Explorer** window, one way to tell that something is odd is that the icon for the **.gif** file is not a gif file icon. Normally, the icon would be one for the particular image editor that is registered to handle that file type. The second two files in the **Explorer** window would not show an extension no matter what setting the "Hide extensions of known file types" switch has.

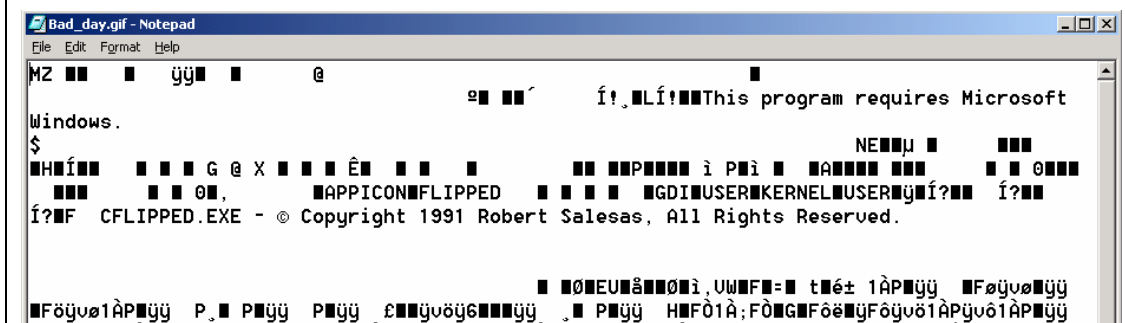
The extension does cause them to have the small arrow in the lower-left corner of the icon which indicates they are a link of some sort. The third file also appears to be a .gif file by the extension but the icon is easily identifiable as belonging to a .pif file.

Directory of D:\TEMP

```
07/29/2002  02:53p      <DIR>          .
07/29/2002  02:53p      <DIR>          ..
07/09/1999  04:38p                4,128 Bad_day.exe
07/09/1999  04:38p                4,128 Bad_day.gif.exe
07/09/1999  04:38p                4,128 Bad_day.gif.pif
07/29/2002  02:52p                387 Bad_day.lnk
          4 File(s)              12,771 bytes
          2 Dir(s)              55,554,048 bytes free
```

If you are not sure of a certain file type, try opening it with the application that is registered to open that file type. Don't double click on the file. Instead, start the application that is registered to open the file and use the File, Open command within the application to try to open it. For example, if the file is supposed to be a .gif file, try opening it with an image editor. If it won't open, it may be something else.

Security Tip: Another way to check out a suspicious file is to open it with a text editor like Notepad. If the start of the file looks like the following, it is an executable file. Note the "MZ" at the start of the file and the "NE" about one third of the way in. These are markers for a DOS program stub that tells you this must be run under Windows and the NE file type of a Windows NT type executable. The second file marker may also be PE for the Portable Executable file type. Other operating systems have similar markers at the beginning of the executable file types.

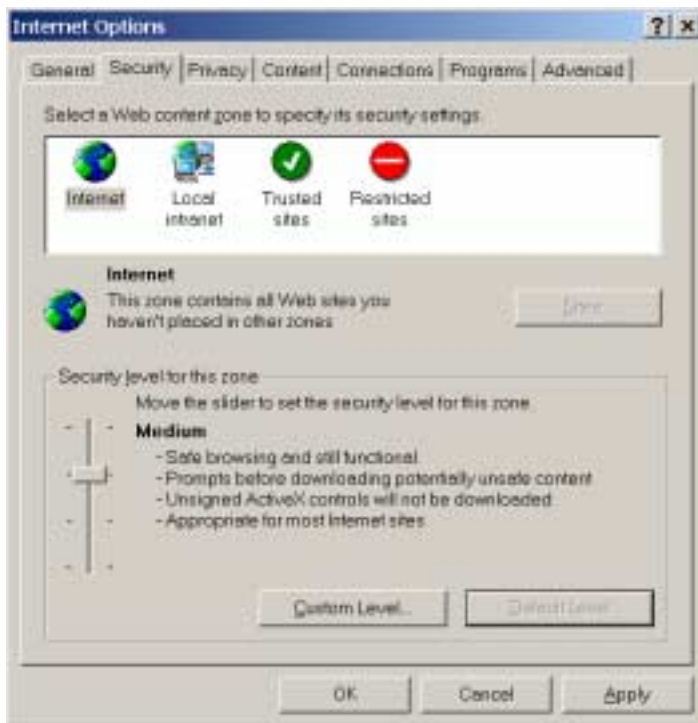


These same restrictions apply for all downloaded files. Be careful what you download. Actually, downloading the file does not infect your system. Executing it after you have downloaded it to your system is what lets the malicious code do its thing.

If you are visiting hacker sites, anarchist's sites, or other sites of dubious character, be sure to have your web browser security settings set to prevent most scripts from running, especially executable files such as Active-X controls, java programs, and so forth. Your web browser should be set to ask before downloading these files and it should check the security certificate the file is signed with. Don't allow unsigned executables to run and don't allow signed executables with untrusted certificates to run. No matter who the

website claims the executables come from, believe the certificate as it is much more difficult to fake.

To control the execution of scripts and executables in Internet Explorer and to enable certificate checking, choose the Tools, Internet Options command and select the Security tab.



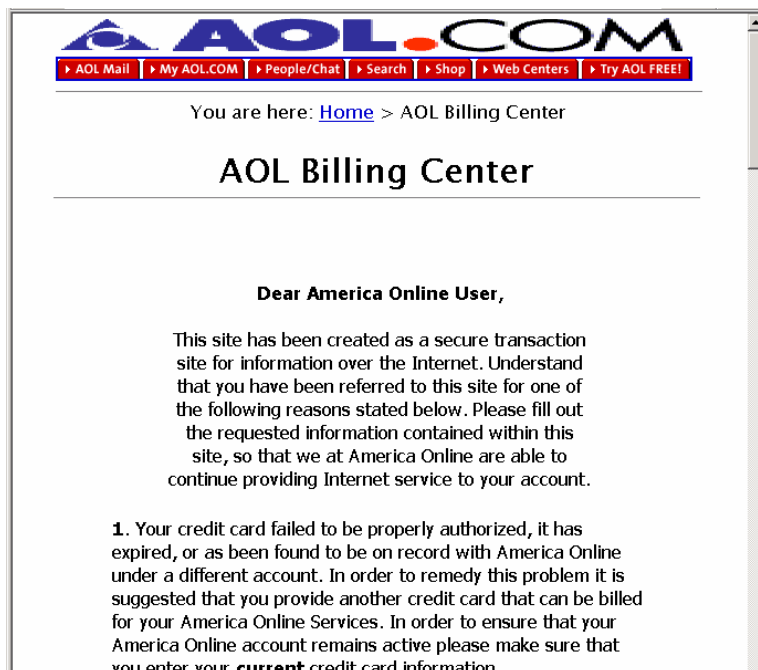
The security level for the Internet zone should be medium or high.

Occasionally we have gotten mail that appears to come from an ISP, telling you that there is a problem with your account and that you need to go to some website to redo your account information. If you go to one of these sites, it appears to be a legitimate website for the ISP and asks for name, address, account name, password, and credit card information. If you fill it in and send it, you have just given an intruder everything it takes to use your account and to charge things on your credit card. If you are ever directed to one of these sites, check the domain name. If the site has no name or the domain name looks strange, don't go there.

For example, AOL users were directed to the site,

<http://216.33.20.4/biz3/AOLTech142/index.html>

Clicking on the link took you to a website that looked like a real AOL site,



AOL.COM

[AOL Mail](#) |
 [My AOL.COM](#) |
 [People/Chat](#) |
 [Search](#) |
 [Shop](#) |
 [Web Centers](#) |
 [Try AOL FREE!](#)

You are here: [Home](#) > AOL Billing Center

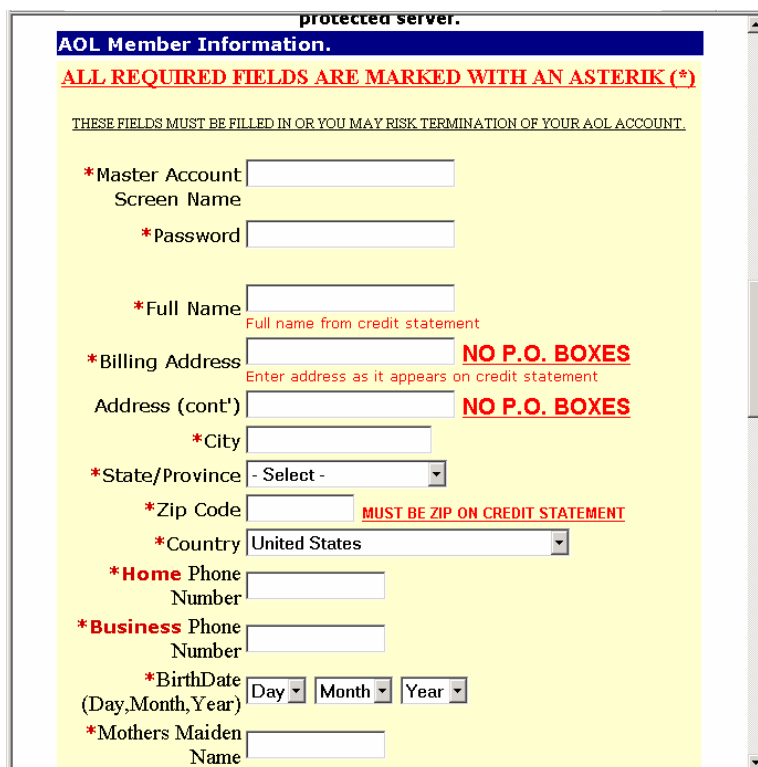
AOL Billing Center

Dear America Online User,

This site has been created as a secure transaction site for information over the Internet. Understand that you have been referred to this site for one of the following reasons stated below. Please fill out the requested information contained within this site, so that we at America Online are able to continue providing Internet service to your account.

1. Your credit card failed to be properly authorized, it has expired, or as been found to be on record with America Online under a different account. In order to remedy this problem it is suggested that you provide another credit card that can be billed for your America Online Services. In order to ensure that your America Online account remains active please make sure that you enter your **current** credit card information.

At the bottom of the message you were asked to fill in a form to reenable your account.



protected server.

AOL Member Information.

ALL REQUIRED FIELDS ARE MARKED WITH AN ASTERIK (*)

THESE FIELDS MUST BE FILLED IN OR YOU MAY RISK TERMINATION OF YOUR AOL ACCOUNT.

*Master Account

Screen Name

*Password

*Full Name Full name from credit statement

*Billing Address **NO P.O. BOXES**
Enter address as it appears on credit statement

Address (cont') **NO P.O. BOXES**

*City

*State/Province

*Zip Code **MUST BE ZIP ON CREDIT STATEMENT**

*Country

*Home Phone Number

*Business Phone Number

*BirthDate (Day,Month,Year)

*Mothers Maiden Name

It looked good, but was all fake. Any information you typed was mailed to an intruder. If you think there is a problem with your account, go to your ISP's website and take care of it there, not at some site listed in an e-mail message from someone you don't know.

Internet rumors are not a source for security information. E-mail messages with patches for all manner of systems are floating around the Internet. In most cases those patch programs are actually viruses, worms, and other malicious code masquerading as security patches. If your system needs a patch of some sort, go directly to the website for the company that is supplying your software to get it.

One habit change that seems obvious at the outset is to simply turn off a system when it is not in use. If the power is off, you cannot be attacked. Why leave a system on 24 hours a day when you don't need to. If you only use your system for 4 hours every evening, turning the system off reduces your risk to $1/6^{\text{th}}$ of the previous value. In addition to protecting your system, turning off the power reduces energy usage and extends the lifespan of your equipment.

6 CREATING AN ELECTRONIC SECURITY PERIMETER

Now that you have patched and configured your existing systems and modified your behavior to improve your security, you need to modify your network to further improve your security. These network improvements are not expensive, and may actually save you money in the long run. The first step is to install a personal firewall between your personal network and your connection to the Internet. The type of firewall you can use depends on how you connect to the Internet and how many machines you have in your home network.

A large percentage of Internet users use a phone and modem to connect to their ISP who then connects them to the Internet. A growing percentage of users have switched to a broadband connection (ISDN, DSL, Cable Modem) to take advantage of the higher speeds. A disadvantage of broadband connections from a security point of view is that they are on all the time. Which means that 24 hours a day, intruders can probe your home network for a vulnerability they can use to exploit your system. While you may be careful, what's to keep a family member from opening a security hole an intruder can use. For example, if a family member turns on sharing without a password to share files between two machines on your internal network they have also opened that system to share files with the world.

Currently, the best way to protect a home network from exploitation of unknown or inadvertent security holes is to add a personal firewall between that network and the Internet connection. The simplest personal firewalls block all incoming connections and allow all outgoing connections. In that way, users within your network can connect to whomever they want but external users can't connect to any internal machine. This still will not protect you from going to a malicious site and downloading a malicious code but it will protect you from people who try to come into your system from the outside.

More complicated personal firewalls actually do some packet inspection to determine the type of content in a connection and to selectively block certain types of content. For example, pornography can be detected and blocked so an internal user can be prevented from viewing it.

A feature of most firewalls is that they use Network Address Translation (NAT) to share a single IP address among several internal users. As most ISPs charge extra for each address that you use, installing a personal firewall can save you money. They will usually save you enough so that you can pay for the firewall in a year or two. Keep in mind though, that some ISPs specifically disallow the use of address sharing.

6.1 SECURITY BARRIER OPTIONS FOR HOME NETWORKING

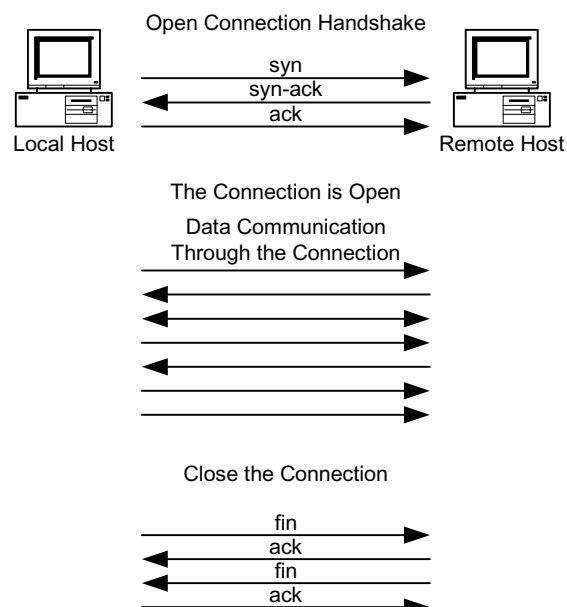
There are several options for creating a firewall between your personal network and the Internet. Different solutions have different strengths and weaknesses and are more or less appropriate for different situations. The two basic kinds of personal firewall are, software and hardware. Software firewalls are programs that run on the computer being protected. Hardware firewalls are small routers that protect a whole subnet. Firewalls can also have

different features such as packet filters, port forwarding, stateful packet inspection, program authorization, remote management, and VPN.

6.1.1 Simple Packet Filtering Firewall

The simplest firewall like program is the packet filter. A *simple packet filter*, as its name implies, looks only at individual packets when deciding to pass a packet or not. Packet filters do not look at the sequence of packets that make up a communication *session*. For example, the **ipfw** program in Macintosh OS X is a simple packet filtering firewall. Because you are filtering only on packets, the ruleset for this type of firewall tends to be a little complex for doing the same thing as a Session Managing firewall (see below). For example, the simplest session managing ruleset is to block all sessions that start on the outside and allow all sessions that start on the inside. Any session involves packets going both directions through the firewall so a packet filtering firewall must look at packets going in both directions and correctly pass or block them to obtain the same connectivity.

To understand how this works, you first need to know how TCP/IP sessions are created and closed. When a system wants to open a new connection to a port on a remote host, it first sends a packet with the **syn** flag set (a syn packet) to the port it wants to open on the remote host. The remote host responds with a packet with the **syn** and **ack** flags set (a syn-ack packet), indicating that the connection is being opened. If a connection cannot be opened for any reason, the remote host sends back a reset packet with the **rst** flag set (a rst packet). If the remote host responds with a syn-ack packet, the local host responds back with an ack packet and the connection is open. Packet traffic then travels in both directions over the connection until the systems are done using the connection. Either of the two systems using the connection can send a close connection packet which has the **fin** flag set (a fin packet). The system receiving it acknowledges receiving the fin packet, sends back a fin packet of its own, and the connection is closed. Any packets associated with the connection that are received after the session is closed generate rst packets.



As an example of firewalling with the **fwvm** packet filter you would start with a rule that allows all outgoing (**out**) packets,

allow ip from any to any out

Next, you want to block all packets associated with sessions starting on the outside but not those associated with any session started on the inside. Because a packet filter does not know which side a session started on, the most you can block are the incoming (**in**) open connection packets (**setup**, the syn packets),

deny ip from any to any in setup

These two rules correctly manage any normal session traffic but are ineffective against scans that do not test for open ports using an open connection packet. For example, the **nmap** tool can be used to scan networks using ack and fin packets. Ack scans scan with the third packet (an ack packet) in the three packet open connection handshake and watch for a rst packet from the port they are scanning. A fin scan does the same but scans with the close connection (a fin packet) packet. Neither of these scans would be blocked by the rules above. If you were to write rules to block either of these packets when they are incoming, you would prevent internal machines from opening connections to external hosts.

This inability to handle sessions is a significant drawback to using packet filters as firewalls.

6.1.2 NAT Router

The next step up is a NAT Router. A NAT router operates using the *Network Address Translation (NAT)* protocol. NAT was originally designed to alleviate the problem that we were running out of IP addresses. NAT uses unroutable IP addresses inside the firewall and routable addresses on the outside.

Security Tip: A part of the IP protocol is a series of address ranges that are designated as private addresses. The addresses in these subnets are unroutable. That is, no router in its default configuration will pass them on so they can only be used within an unrouted network. These addresses can be used over and over again on the Internet because packets using these addresses as a destination will not be routed by a router. The unroutable addresses are (see RFC 1918),

10.x.x.x	One class A network.
172.16.x.x through 172.31.x.x	16 Class B Networks
192.168.x.x	256 Class C Networks

A NAT Router maps a single external address to multiple internal addresses. When an outgoing connection attempts to open, the router rewrites the packet header to have the router's IP address in the source field and an open port on the router as the source port. This port is then linked to the port on the internal machine that opened the connection.

Packets coming back from the destination machine to the mapped port are rerouted to the mapped port on the internal machine.

Security Tip: More expensive NAT Routers can map multiple external addresses to multiple internal addresses but that capability is not generally available in personal firewalls.

As far as the internal machine is concerned, it is connecting directly to an external machine. It does not even need to know that the address translation is going on. Because of the way that it works, multiple internal machines can share the same external address. This allows you to have multiple machines on your internal network but only need purchase a single IP address from your ISP.

Note: Some ISPs encourage the use of NAT while others discourage it and require that you buy an IP address for every machine that you place on the network. Be sure to check your user agreement before implementing NAT.

An external machine can only see the single external address of the NAT Router. It cannot see any of the internal machines directly because packets with those unroutable addresses are not routed. If an external machine attempts to open a connection to an internal machine, the NAT based firewall blocks that attempt.

Another benefit of NAT is that if the internal network is accidentally directly connected to the external network, systems beyond the first router still cannot directly connect to any of the internal machines because the unroutable addresses used by the internal machines will not be routed to them.

A problem with NAT is that internal servers cannot be made accessible to clients on the outside. By its design, NAT blocks sessions that start on the outside, which prevents an external client from connecting to an internal server.

Other problems with NAT include the use of protocols that use multiple ports and to peer to peer communications. For example, the ftp protocol uses two data paths. One outgoing connection to the server on port 21 for commands and a separate incoming connection from the server on port 20 for data. A NAT Router by its design blocks that second data path.

Peer to peer communications generally start with the two peers connecting to a server. The server then passes the remote IP addresses and ports of the two peers to each other and expects them to communicate directly after that. NAT on a personal firewall will see the incoming communications but because the IP address of the remote system is different from when the communication channel opened, NAT blocks the connection. Peer to peer communications are primarily used in peer to peer computer gaming and is not generally a problem for company communications.

6.1.3 Stateful Packet Inspection Plus Port Forwarding

To handle the problems with simple NAT routers, personal firewalls implement *Stateful Packet Inspection*. A firewall implementing stateful packet inspection understands the protocol as well as the simple routing information in a packet and uses that to allow protocols through a firewall rather than single, outgoing sessions. Most home firewalls need to understand only a few special protocols such as ftp as most connections are handled correctly by NAT.

In addition to Stateful Packet Inspection, most home firewalls also allow *port forwarding*. Port forwarding is used when you want an internal server to be accessible to machines on the outside of the firewall. Port Forwarding, which is also known as an *application proxy* works by mapping a port on the outside of a firewall to a port on a machine on the inside of the firewall. Incoming packets to the port on the outside of the firewall are redirected to the designated port on the internal machine to allow a session to be created that starts on the outside of the firewall.

For example, if you want a web server to be accessible to external users, you would map port 80 on your internal server to port 80 on the outside of the firewall. All connections to port 80 on the firewall are then passed to port 80 on the internal web server.

A downside of the simple NAT routers is that you cannot have two internal web servers both operating on port 80. You can have them on different ports, but not both on the standard port 80. More expensive firewalls allow multiple external addresses to be mapped to multiple internal addresses, allowing you to have any number of servers operating on the standard ports accessible to external users.

6.1.4 Packet Filtering

Packet Filtering is the next step up in firewall complexity (note that this is different from a simple packet filter that looks only at single packets.) Using stateful packet inspection to control the sessions, packet filtering looks at the contents of the packet stream instead of just the packet headers. Packet Filtering can be designed to look for anything within the packet stream from pornography to hacking attempts.

Packet filtering in personal firewalls currently detects only a few specific things. Another caveat with packet filtering in personal firewalls is that it must be kept up-to-date with a subscription service.

For example, the Netgear FR314 Firewall Router can block the following things,

- Active-X controls
- Java applets
- Cookies
- Web Proxies
- Web/Gopher/FTP content (profanity, nudity, violence, etc.).

As another example, the SofaWare S-Box can control the following things,

- Web/Gopher/FTP sites based on content (profanity, nudity, violence, etc.)
- Viruses in e-mail messages

Both of these require a service to provide the lists of sites to block and to do the virus scanning. Both the Netgear and SofaWare products have upgradeable software so the types of inspections could expand or change in the future.

Security Tip: Many personal firewall products claim they do stateful packet inspection and packet filtering but the things they look for and the amount of detail they can examine is often quite different. Be sure to check the specifications to see what can be examined within a packet stream. Note that you may need to get a copy of the setup manual to see what can really be set in these products as the marketing descriptions are often ambiguous.

6.1.5 Program Authorization

A capability that is unique to the software firewalls is *program* or *file authorization*. What this does is to define a list of programs on the host computer that are allowed to connect to and send information to the Internet. The primary use of this feature is to prevent viruses and worms on the host computer from attacking others on the Internet and to block *backdoor programs* that have been inadvertently installed on a system. It can also warn you when programs that you would not expect to be connecting to the Internet are attempting to do so. For example, this would block some spyware and adware programs that are trying to install advertising on your system or that are trying to upload your browsing habits to a remote server.

Program authorization cannot be done by hardware firewalls, but some hardware firewalls with stateful packet inspection and packet filtering can be given rules to recognize and block connections to known problem sites, connections from known backdoor ports, and outgoing virus infected e-mail.

6.1.6 Remote Management of Firewalls

Most of the hardware firewalls allow for remote management of the firewall. Inexpensive firewalls allow only the setting of network information such as IP addresses and network masks. More expensive firewalls allow the setting of all of the firewall rulesets. Remote management can either be a service provided by an ISP, by a company paid to manage the firewall, or by an employer who is managing employer owned equipment at an employee's home.

Be careful when setting up access for remote management. Make sure that only the remote management service can manage your firewall by setting appropriate address restrictions and user authentication. How you do this is dependent on the particular firewall. The simplest home firewalls require a username/password login plus they limit the connection to only the IP address of the manager's machine.

There are a few high end hardware home firewalls that are actually low end enterprise firewalls that run the same software as the enterprise firewalls just in a slower, less capable box. These systems are designed with remote management in mind, and in most cases use the same management software as the enterprise firewalls. Home firewalls of this type are the SofaWare S-Box which runs Firewall 1 and the CISCO PIX-501 which runs PIX.

6.1.7 Wireless Home Networks (WLAN)

Most of the hardware firewalls have 10/100 Ethernet ports (RJ-45) on the internal network side. A few have a wireless access point in addition to the Ethernet ports. Wireless is very convenient, especially if you live in a house that is not wired for computers or that cannot be easily wired. Using wireless, you can move a computer to any room in the house and still be connected to the Internet. You can also carry a laptop to the neighbor's house and use it there. Some examples are the LinkSYS BEFW11S4, and the Netgear MR314 shown below.



Security Tip: Not all wireless is the same. While wireless systems were supposed to be compatible across different manufacturers, the current crop of hardware devices is not. Be sure the network cards and wireless access point you buy will work together.

We tested one home *wireless access point* and were able to successfully connect to the network up to nearly a city block away. Herein lays the biggest risk of using wireless. Unless they are properly configured for security, anyone within range of the wireless access point can connect to your home network and use your Internet connection.

Out of the box, a wireless access point is easily exploited. An intruder need only get within range and turn on his computer. The wireless access point and the intruder's wireless card negotiate the connection and the IP address, and he is in.

Even with encryption turned on, flaws in the encryption algorithm (WEP) make it easy to break, making the protected packets readable. Newer versions of the encryption algorithm and stronger keys are becoming available so newer wireless systems will be more secure. Old wireless systems may be able to do a firmware upgrade to be able to use the new standards. It is even more important here to make sure the wireless access point and the wireless cards you buy are compatible and can both handle the higher levels of encryption.

Properly configuring a wireless access point involves,

- Keeping the signal within your property lines
- Changing the Service Set Identifier (SSID)
- Setting the channel
- Turning on Wireless Encryption, Wired Equivalent Privacy (WEP)
- Turning on Access control by MAC address

The first step in securing a wireless network is to try to move the wireless access point as close to the center of your property as possible. Then, reduce the power of the transmitter to keep the usable area within your property lines. Reducing the transmitter power may involve turning a knob or reducing the size of the antenna.

The *Service Set Identifier* (SSID) is the name by which this wireless access point is known. When setting up a system, it should be changed to something other than the default. While this name can be sniffed with a wireless sniffer, changing its name makes it more difficult for an intruder to gain access to your system. Changing the channel you operate on has the same effect in that the available channels can be sniffed but changing them makes it more difficult for an intruder.

Wireless encryption should be turned on. Even the older, vulnerable encryption standard provides some protection. Without WEP, access to your access point is only controlled by the MAC address described later. With WEP turned on, each machine needs to have an encryption key that matches that set in the access point. You should use a shared secret in a small, home network.

The encryption level controls the difficulty with which an encrypted message could be decrypted. The original WEP encryption specification has a flaw that makes it easy to decrypt. Newer systems allow larger encryption keys to significantly increase the difficulty with which the encryption can be broken. Using larger encryption keys also degrades the network performance so use the highest level of encryption that you can that does not significantly degrade the network performance.

When you turn on access control by MAC (Media Access Control) address, you enter the MAC address of the wireless cards that are going to be allowed to connect to your system. While the MAC address can be forged, an intruder would have to know one of the allowed MAC addresses in order to gain access to your system.

6.1.8 VPN Options

Virtual Private Network (VPN) options are available (for an additional fee) on some of the higher priced hardware, home network firewalls. They are also available as a software solution running on a single machine. Hardware VPNs create an encrypted pipe from your home network through the Internet to a company VPN server. It makes the firewall and the systems behind it appear to be on the company network, making it relatively easy to transfer files and access services. As the pipe is encrypted, all communications through that pipe are protected. A software VPN works similarly, but applies only to the machine running the software and not to your whole home network.

Security Tip: Not all VPNs are the same. Make sure that when you buy a VPN solution that it is compatible with the VPN server that you want to connect to. VPNs also come as clients and servers. If you want to connect two subnets together through a VPN, one must be a client and one must be a server.

6.1.9 Software Firewalls

A software firewall is actually a program that runs on your home computer. This program operates as a network service and watches all connections to and from your system from the network. Most incoming connections are blocked unless you specifically allow them in. The allowed outgoing connections are determined by the particular firewall used and can be configured to match your needs.

Software firewalls are the least expensive of the personal firewall products, and typically run in the \$50 range. Software firewalls work with most network connections including those that use a telephone and modem and those that connect directly to a network using a network card. A network connection can be shared with other systems on your internal network if your operating system supports NAT (Windows 98 and later and most UNIX like systems). Some software firewalls can also do program authorization, which cannot be done by hardware firewalls.

Windows XP has a built-in software firewall known as the Internet Connection Firewall. Enable this firewall with the Network Connections control panel. Select the connection you want the firewall on and choose the File, Properties command, Advanced tab. Check the box “Protect my computer and network by limiting or preventing access to this computer from the Internet.” This setting turns on a firewall that blocks all incoming connections and allows all outgoing connections. To allow incoming connections to services you want to make available (such as a web server) to someone outside of your computer, click the settings box and select the service you want to let in. Several common services are already defined or you can create custom entries if you know the port number for the service you want to make available.

In addition to a software firewall, Windows XP has a file authorization capability known as the Software Restriction Policy. With the Software Restriction Policy, you determine which software is allowed to run on a system. Software that is not on the allowed list will not run when the policy is enabled. This is useful for preventing viruses and worms from running on a system because if a virus is not authorized, it’s code will not be allowed to run on a system. A problem with this tool is that there are no predefined policies for standard software programs. You must create all the policies yourself by selecting the programs you want to allow to run. While this isn’t difficult, it is time consuming if you have a lot of programs on your system that you want to authorize. A description of how to turn on this capability and a list of the settings and of how to create the rules is available from the Microsoft website.

**[http://www.microsoft.com/windowsxp/pro/techinfo/administration/
restrictionpolicies/SoftwareRestrictionPolicies.doc](http://www.microsoft.com/windowsxp/pro/techinfo/administration/restrictionpolicies/SoftwareRestrictionPolicies.doc)**

The Macintosh OS X system also has a simple software firewall built into it known as **ipfw**. However, as mentioned previously in section 5.3.3, this is a simple packet filter and does not know about sessions.

Problems with software firewalls are that they run on your system and thus use up some of your computer resources. Heavy scanning of a system containing a software firewall can perceptibly slow that system. If you are using NAT to share your modem connection, all the communications for all the systems on your network must go through the system that is performing the NAT and firewall functions. If you have a lot of internal systems and they are all actively connecting to the Internet, the system running NAT and the firewall can be perceptibly slowed.

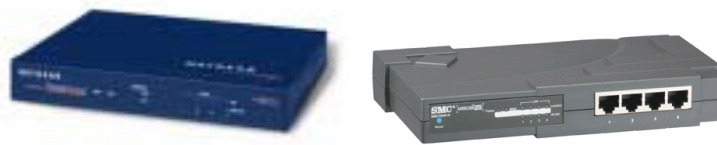
Another difficulty with software firewalls is that they run on your computer and examine a packet of information from the network after that packet is already on your system. If the vulnerability is in the *TCP stack* of your system it may be exploited before the software firewall can detect and block the packet.

6.1.10 Hardware Firewalls

Hardware firewalls are small network appliances that are optimized to control the routing of packets between an internal and an external network. The most basic hardware personal firewall costs under \$100, provides NAT, some stateful packet inspection and port forwarding to a single subnet of computers. In this basic configuration, it blocks all incoming connections and allows all outgoing connections. They can also do port forwarding so that a few services can be made available to systems outside of the home network. Many of these basic units do not even call themselves firewalls. Instead, they are described as NAT routers or routers with firewall capabilities. For most home networks, this is more than sufficient to protect that network. The biggest limitation to these systems is that most cannot do peer-to-peer networking to peers that are outside of the home network though that is changing. Some examples are the D-Link DI-701, the Netgear RT311, and the SMC7004ABR shown below.



In the \$100 to \$300 range, you start adding features such as packet filtering, remote management, wireless, and VPN. Other features include a print server, fail over to a modem if the broadband connection fails, and parental controls (part of packet filtering). Some example are the Netgear FR324 and the SMC7004FW shown below.



At the high end in the \$300 to \$500 range are the baby enterprise firewalls. These home firewalls run the same software and use the same management schemes and rulesets as the enterprise level firewalls. Some examples of these are the Sofaware S-Box which is a Firewall 1 firewall and the CISCO PIX-501 which is a PIX firewall. Home firewalls of this type are of special interest to companies who want to have remote control of a company firewall installed in an employee's home. They can be configured to prevent a home user from overriding security and putting the company at risk.



Most of these systems come with 10/100base-T LAN ports (internal) and a 10base-T WAN port (external). This is because most cable modems and ISDN modems only operate at 10base-T levels. Some of the newer units have 10/100base-T WAN ports so they can be used to firewall a single machine or small subnet from a larger network.

Security Tip: Some hardware personal firewalls allow as many hosts behind the firewall as you want (within the limits of the hardware to handle) while others license some maximum number of hosts (like 4 or 5). Be sure the firewall you buy can handle the number of hosts that need to use it. Note that only hosts that need to communicate through the firewall need to be included in that count. Systems such as printers that do not need access outside of the firewall are not counted.

The specifications, capabilities, and costs of hardware personal firewalls are changing rapidly. During the time it took to write this report, the prices of many systems have dropped by about 1/3 and many new systems and features have appeared.

6.1.11 Tradeoffs

The tradeoffs between the hardware and software firewalls are in the following table.

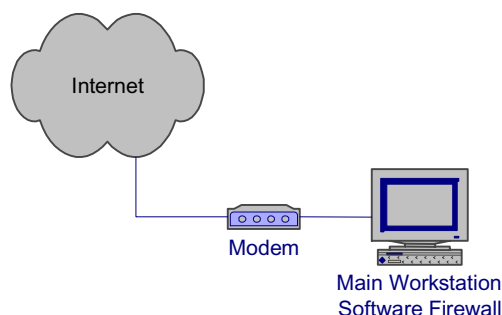
	Software Firewall	Hardware Firewall
Price	Less expensive. Most are less than \$50.	Slightly more expensive. \$50 to \$100 for a NAT router; \$100 to \$500 for additional features.

Reliability	Less reliable. Runs on the protected system and so depends on the software and the reliability of the protected system.	High reliability. Single mission hardware units. Much simpler software design.
Attackability	Can be compromised along with the multi-mission system they run on.	Extremely difficult to compromise. Single mission hardware units with few “features” to exploit.
File Authorization	Yes, available on some products.	No. File authorization can only be done on the protected host.
Stateful packet inspection	Yes	Yes.
Packet Filtering	Yes, depends on the product.	Yes, depends on the product.
Mail antivirus scanner.	No. Can be done with a separate package.	Yes. On some of the units with packet filtering. Must be updated regularly. Some send the mail to a separate server for scanning.
VPN	No. VPN is implemented with a separate software package on the protected host.	Yes. On some models.
NAT	No, but some operating systems provide that feature independent of the firewall.	Yes.
Simple Packet Filter	Yes, it is built-in to some operating systems.	No.
Remote Management	Yes. Some are.	Yes. Most are.
Updatable	Yes.	Yes.
Attack detection.	Yes, but must be updated regularly.	Yes, but must be updated regularly.
Modem connection	Yes. These work with modem or Ethernet connections to the Internet.	Yes. Most of these are Ethernet only but a few units allow failover to a modem connection.

Slows workstation	Yes. The degradation depends on the network load.	No. Workstations actually work faster because the internal network is quieter.
Internal Servers	No.	Yes, one server allowed per port.
Peer-to-peer connections.	No.	Yes, depends on the unit. Less expensive units do not support it.
Other Options	No.	Print server, modem fail over, wireless.
100-baseT on the WAN (outside) connection.	Yes. Depends on the computer's Ethernet card.	Yes. On some of the newer units only. Older units are only 10-baseT on the WAN connection.

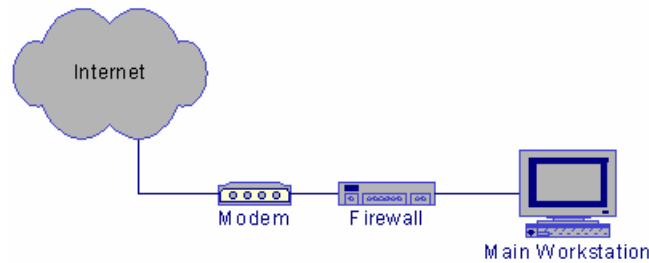
6.2 PROTECTING A DIAL-UP CONNECTION

The simplest and most common home network consists of a single computer with a dial-up modem. A software firewall is the most reasonable solution for this system. A software firewall with file authorization would also protect other systems in the event that your system was compromised by a worm or virus.



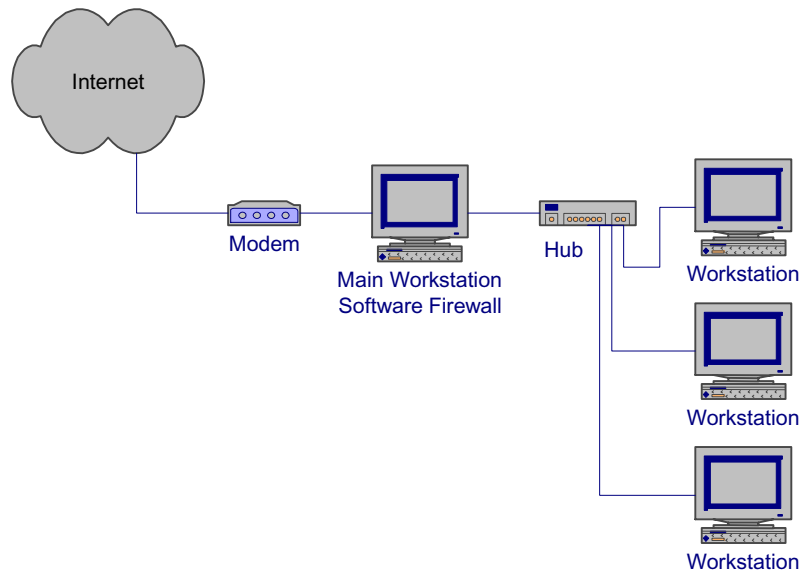
Be sure to disconnect a dial-up connection when you are not using it. This not only frees up the telephone line it reduces your risk to attack by limiting your exposure to the Internet.

There are a few hardware firewalls that could be used in this situation but most are designed with an Ethernet WAN connection. We have seen some with a built-in modem and others with serial ports that can be plugged into an external modem and used for the Internet connection. You would need to check these carefully to be sure that they work with your ISP.

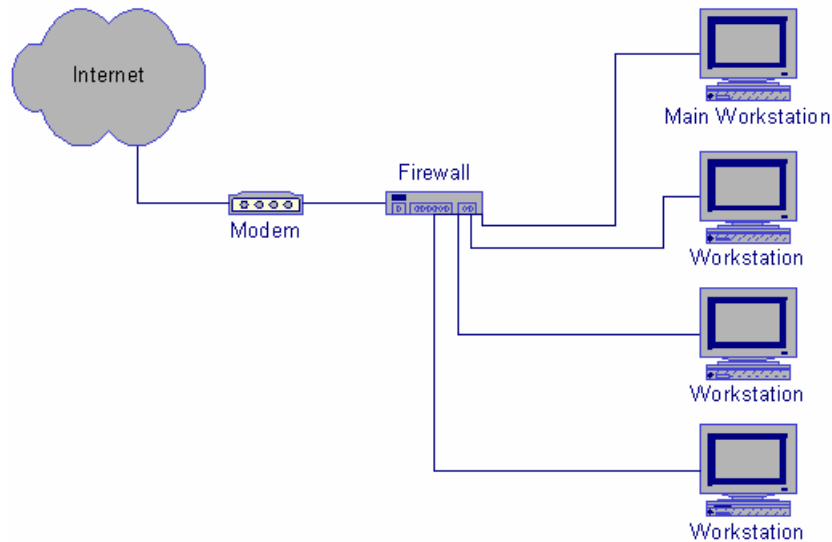


6.3 PROTECTING A SMALL NETWORK WITH A DIAL-UP CONNECTION

To protect a small home network that consists of two or three systems and a dial-up connection to the Internet, you have a couple of options. If you have a relatively fast workstation that can operate the modem and that can provide the NAT connection sharing (such as Windows 98 or later) for the rest of your network, you can use a software firewall on that workstation to protect it and the other systems connected to it through its Ethernet port. To make this work, you need an Ethernet port on all the systems and a small hub or switch to connect them together. The fast workstation then handles the connection sharing, firewall, and modem control.



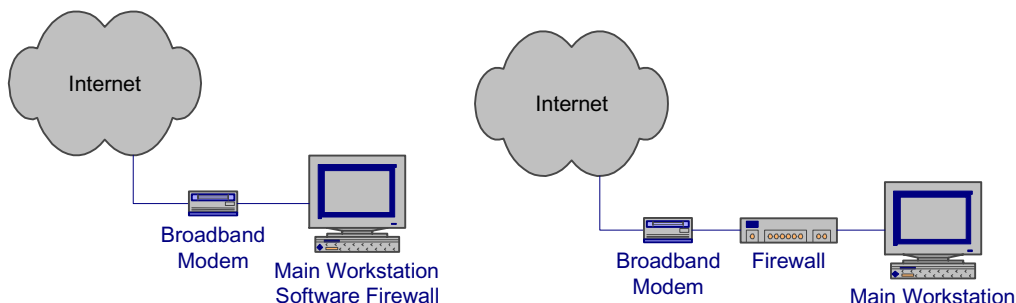
Another option is to get one of the hardware firewalls that have a built-in modem or that have a serial port designed to be connected to a modem. The hardware firewall then controls the modem as well as performs connection sharing with NAT and network protection. Be sure the modem-firewall configuration will work with your ISP.



In both situations, you could put a software firewall with file authorization on each of the internal systems to prevent them from spreading a worm or virus.

6.4 PROTECTING A SINGLE SYSTEM WITH A BROADBAND CONNECTION

A single system connected to a broadband network can use either a software or hardware firewall. If you are planning to add more systems to your home network in the near future, you should consider one of the hardware firewalls as it will allow you to add systems without having to buy more IP addresses if your ISP allows it.



A hardware firewall is also useful if you occasionally bring home a company laptop and need to put it on the Internet. Most hardware firewalls and software NAT servers use DHCP to provide network addresses to connected systems. With the laptop set to use DHCP to get its address, you need only plug it into one of the LAN ports of the firewall to get connected. All the network settings are done through DHCP.

If you need to connect one system through VPN to get to a company site, use a software VPN solution on the system that needs to connect to the site. To put the whole subnet on the VPN connection to the company site, you can use multiple software solutions, a software solution on the main workstation if you are using a software firewall or a

hardware solution if you are using one of the hardware firewalls with a VPN option. Before you put your whole home network on the VPN connection consider if all your home computers need to be on the company network. If other people in your household are using the home network for personal items, you should only put the one system that needs to connect to the company network on the VPN.

6.5 PROTECTING A HOME NETWORK WITH A BROADBAND CONNECTION

When you are protecting a home network consisting of multiple machines, a hardware firewall is the best option. The hardware firewall offloads the firewall and networking duties from your main workstation and handles them all in the firewall. The hardware firewall quiets the whole network so your main workstation does not have to spend time discarding packets that do not apply to it. The single shared connection easily pays for itself in a year or two.

You may want to add additional protection for systems that are more at risk for getting a virus or worm. For example, a system where the primary user likes to double click things and go to hacker sites. You can add a software firewall with program authorization to the at risk system to protect other systems from an inadvertent worm or virus infection, or from an accidentally installed backdoor.

You might also want to consider a hardware firewall with a built-in wireless switch if you move around a lot or don't have wires where you need them. Keep in mind though that hard-wires are faster and more secure than a wireless solution.

6.6 PROTECTING A HOME NETWORK WITH WIRELESS NETWORKING

In addition to the protections described in the previous sections, a home network using wireless networking also needs to protect the wireless part of the network from intruders. Most home wireless network access points are NAT routers with both wired and wireless connections for the internal LAN. Unfortunately, the wireless part of the network has significant security problems.

- Wireless routers in their default configurations have no security turned on. Anyone within range of the transmitter can connect to your network, get an address, and begin using that network's Internet connection.
- The Wireless Equivalent Privacy (WEP) as deployed in older systems is flawed. The encryption key is too small and other implementation problems make it relatively easy to break. Exploit scripts exist that can easily break the encryption and gain access to the packet contents.

Newer wireless routers are available with better encryption and a new Wireless Equivalent Privacy is being developed (WEP2) so future wireless routers and old routers that can have firmware upgrades will be much more secure. See the section on Wireless Access points for configuration information. Check with the manufacturers of home wireless networking products to see what improvements there are as this technology evolves.

7 USE PROTECTED CONNECTIONS BETWEEN HOME AND WORK

When using a home computer to access company resources, be sure to use a protected connection between your home and the company networks. Dial-up connections and ISDN are reasonably well protected if they go directly to a company network. This is because they are point to point connections that do not share bandwidth on a normally accessible public network. Note that this does not mean that they are inaccessible, only that they are less public than things like cable modems. If these connections go first to an ISP and then through the Internet to the company network, they are not well protected.

Protect Internet communications to a company network using some type of encryption. At a minimum, your login and password must be protected, either with encryption or with a one-time password scheme. Protecting the login prevents an intruder from being able to use your login to access the company network but does not protect any of the other data passed between your computer and the company network as you work. Even if you are using a one-time password scheme to protect your login, if you are using an unprotected communication protocol such as telnet to connect to a company network it is possible for an intruder to capture your connection and use it to access the company network. An intruder does this by analyzing the unprotected traffic between you and the company network and then inserts his packets in place of yours to take over the connection. As he does this after you have authenticated, he does not need to authenticate to get in.

A better way to protect Internet communications to company networks is with encryption of the communication channel. Encrypted communications channels include SSL (Secure Socket Layer) encryption used for secure web servers (https), VPN (Virtual Private Network) encryption, and SSH (Secure Shell).

SSL encryption is built into most modern web servers and can be configured to require high-encryption (128 bit keys) connections. The slight slowdown due to the encryption is hardly noticeable in systems using current technology. SSL encryption opens an encrypted connection first, before authenticating the client so that the username and password of the client pass through the encrypted connection. Note that in a normal web connection the username and password are passed nearly in the clear. They are protected by a simple hash that is there only to disguise the username and password.

A Virtual Private Network (VPN), discussed earlier, creates an encrypted pipe from a user's system to a subnet. The user's system then appears to be on the remote subnet and all communications go through the encrypted pipe.

Secure Shell (SSH) opens an encrypted pipe between one system and a shell on another. The shell is a command line interface on the remote system with all communications going through the encrypted pipe. Other protocols, such as X windows, can be passed through the encrypted pipe to create a protected GUI interface. SSH also includes secure copy, SCP, which can be used to securely transfer files between systems.

Security Tip: Simply using one of these encrypted links does not assure you that the information is being fully protected. These and similar systems strongly protect the data path between the user's machine and the company network. When using these, the weakest links are the machines at the end points of the connections. If a user's system has a back door installed, an intruder can see everything that happens on that system including the communications through the encrypted link.

8 POLICY CONSIDERATIONS RELATED TO WORKING FROM HOME

Companies that allow their employee's to work from home derive many benefits, not the least of which is more use of an employee's time. An employee who can login in the middle of the night to check a process doesn't need to come into work to do so. The employee sees a more effective use of his time as he can do a quick check of a process without having to drive into work and can go back to whatever he was doing at home. Employee's who are working at home in the evening can get access to files they need for their work instead of having to put the work off until the next day.

The downside of working at home has been highlighted in this paper in that each home connection is another uncontrolled or semi-controlled pipeline behind the company firewall. While the firewall is maintained by security professionals, the home machines generally are not. To assure themselves that they are adequately managing the risk of home connections to a company network, the company needs a home use policy that spells out the requirements for that home connection, both for the employee at home and for the security staff. The policy should result in a user agreement that the home user can use to make sure he has not missed anything in protecting his system. The home user should also see this policy as improving the security of his personal resources and not a hindrance on his getting work done.

This section contains some of the items that should be considered when formulating a home use security policy.

8.1 COMPANY COMPUTER AT HOME

When a company computer is used at home to access company resources, control of that computer is more strongly in the hands of the company security staff. They can largely control the contents of the computer and manage it for required updates and security software.

Company policy for such a machine can be much stricter than for a machine that is owned by the employee but should not be so strict that the employee refuses to use it. Risk management and cost-benefit analysis comes into play here when deciding the requirements for home use. Keep in mind that you are using a portion of an employee's home at no cost and getting the use of that employee on off hours, also likely at no or little cost. You are also making it more convenient for an employee to do his work.

Use of the system for non-work related computing will likely already be spelled out in existing company policy. Most government owned systems cannot be used for personal use except in the most minimal way, such as occasionally sending an e-mail message.

Employee requirements for using and protecting the system needs to be spelled out in the policy and the user statement. The amount of personal use allowed also needs to be spelled out. Banners are generally needed to remind the users of the system about the personal use policy.

8.2 PERSONAL COMPUTER USED TO ACCESS COMPANY RESOURCES

The policy for using an employee's personal computer for access to a company network is more problematic. You cannot generally tell a person what he can and cannot do with his personal computer in his off time. But, a company can expect some level of security in a system that is allowed to connect to a company network. An employee should feel that he has obtained some benefit for adhering to the policy beyond being able to go to work in the middle of the night.

Some things to consider are:

- The company does not have to buy and maintain a computer for the employee
- The employee has the convenience of using a system he is familiar with
- The employee does not have to figure out how to store a second computer and monitor in his home
- The company has less control over the use and maintenance of this system
- The company does have some expectation of a minimal level of security for a system that is going to be used to connect to a company system
- If the employee sees the benefit to himself for maintaining the security of his home system he will be more likely to maintain it in a secure manner

Again, the usage requirements need to be spelled out in the policy and user agreement so the employee knows what he is getting into before he allows his personal computer to be used for company business.

8.3 MAINTAINING THE SYSTEM

Maintaining the system consists of initial installation and configuration combined with periodic maintenance to install updates and check configuration settings.

8.3.1 Company Owned System

For a company owned system, the company has full control over the system and has the responsibility to do the maintenance. If the computer is a laptop, it can easily be brought in occasionally for maintenance and updates. If it is a desktop machine, this becomes problematic and the security staff may need a way to remotely manage the system or even do the maintenance in the employee's home.

System maintenance is less of a problem today than it was a few years ago. With Windows Update and similar products for other operating systems, machines automatically have security updates installed as soon as they come available. The same is true for antivirus software that can be configured to automatically download updates on a regular schedule.

8.3.2 Employee Owned System

Maintaining a system that is not owned by a company is more challenging but most employees would welcome a company's assistance in maintaining their systems. A

company can provide a knowledgeable person to answer questions related to maintenance and security configuration. They can also provide security and maintenance bulletins to the employees at little cost to the company as these would be the same bulletins that are used within the company to maintain internal systems.

Current home systems are largely self maintaining after the initial configuration. The company can provide the user with configuration information, updates, antivirus software and updates, firewalls and other software and hardware that enhances the security of the user's system. If the user sees sufficient benefit to himself for using these items, he will likely use them.

8.4 ANTIVIRUS SOFTWARE

Most companies already have a site license for antivirus software. Company owned computers should be required to have this software installed and running at all times. Employee owned systems can be given the benefit of this site license at little cost to the company as an employee's system also needs to be protected at all times, not just when he is connected to a company network.

8.5 VPN SOFTWARE

One thing a company should provide for remote access to a company network is a VPN server and VPN clients for all remote users. This is a minimum requirement for most remote situations to protect the remote login and the data in transit. Many current generation routers provide a VPN server capability and VPN clients are available as software programs for individual machines.

8.6 COMPANY PROVIDED FIREWALL

Like antivirus software, a company can provide a firewall to an employee for a small cost. Also like the antivirus software, the firewall protects a system at all times, not just when the system is connected to a company network. Which firewall you use depends both on the size of the network and the amount of control a company wants to exert.

A company can easily supply a software firewall for an employee's computers. That firewall will significantly improve the security of a system but does not give a company much control over if the firewall is turned on and the level of protection being afforded by the firewall. Using one of the less expensive hardware firewalls also provides an employee a considerable amount of protection for his home machines but does not give the company any control over the protection.

Using one of the high end hardware firewalls such as the S-box and the CISCO-501 gives the company control of the firewall and its policies. Using remote management software, a company can change the firewall policies to counter a new threat, however that does come at a cost. The company must now take over the management of these firewalls. Scaling is not a problem here as the firewall remote management software allows you to configure one policy and apply that policy to all the firewalls. One thing this does do is assure the company that the firewall is in place and the rule set is as specified.

Before committing to remote management of firewalls, a company needs to consider if the cost is worth the benefit. The default policy for most hardware firewalls is to block all incoming connections unless a user has turned on port forwarding. Block all incoming connections prevents most attacks from occurring. Remote logging is useful in that it tells you what kinds of attacks are being attempted on an employee's computer. This might give you a heads-up on an attack on a company computer.

8.7 SCANNING AND TESTING

After a system has been setup and configured, it needs to occasionally be tested to assure you that the system has been configured according to the company specifications. Testing of this type can be done by running a program on the home system that checks the various security settings.

Another type of testing is vulnerability scanning. Vulnerability scanning is done to assure yourself that the security patches have been done correctly and that the vulnerabilities have been removed. Vulnerability scanning is done with software like ISS and is usually done remotely to an employee's system.

9 CONCLUSIONS

Home networks are often targeted by intruders because they are plentiful and they are usually not well secured. While company networks have departments of professionals to maintain and secure them home networks are maintained by the homeowner who may know little about network security matters.

If connections are going to be allowed from a home network to a company network that home network must be secured to insure that it is not opening up the company network to intruders. Securing home networks involves many of the same operations as securing a company network.

- Patch and maintain systems
- Securely configure systems
- Eliminate unneeded services
- Protect remote logins
- Use good passwords
- Use current antivirus software
- Moderate your Internet usage habits

Most of these items do not take a lot of work, but require more awareness of the potential risks involved in not doing them or in doing them incorrectly. Of special interest here for most home systems is to insure that file sharing is disabled or has been well protected with good passwords. Open shares can make a system accessible to everyone on the Internet. It is also how many current computer worms spread themselves.

In addition to maintaining the systems in your home network, you significantly improve security by adding an appropriate software or hardware firewall. For home networks with more than one system, the hardware firewall solution can pay for itself in a couple of years through savings in the number of IP addresses you must buy.

Company policy and the user agreement should be very clear on the requirements for connecting a home machine to a company network. They should be written to encourage an employee to apply the same requirements to all his systems by supplying the assistance, knowledge, and tools he needs to do so.

Lastly, home users should keep in mind that home network security is not a “DOE only” activity; don’t forget to help your family and friends do the same. The fewer networks and systems that are vulnerable to intruder activity the better the Internet as a whole will operate.

APPENDIX A – AVAILABLE SOFTWARE FIREWALLS

The following is a list of software firewall products with links to their websites. This list is not complete. Links to reviews of many of these products are available on <http://www.firewallguide.com/>.

BlackICE	http://www.iss.net/
CheckIT	http://www.smithmicro.com
Deerfield	http://dpf.deerfield.com/
eSafe Desktop	http://www.ealaddin.com/
eTrust EZ	http://www1.my-etrust.com/
Firekeys	http://softappco.com/
Freedom	http://www.freedom.net/
GuardWall	http://www.fail safetechnologies.com/
HackTracer	http://www.sharptechnology.com/
Internet Firewall 2000	http://www.digitalrobotics.com/
Kerio	http://www.kerio.com/
Look'n'Stop	http://www.looknstop.com/
McAfee	http://www.mcafee-at-home.com/
Mindsoft	http://www.mindsoftweb.com/
NeoWatch	http://www.neoworx.com/
Norman	http://www.norman.com/
Norton	http://www.symantec.com/
OutPost	http://www.regnow.com/
PC Viper	http://www.pcviper.com/
pcInternet Patrol	http://www.isa-llc.com/
Preventon	http://www.preventon.com/
Privacyware	http://www.privacyware.com/

SecureUp	http://www.secureup.com/
Sygate	http://www.sybergen.com/
Sygate Pro	http://www.sybergen.com/
TermiNet	http://www.gis-secure.com/
TGB:BOB!	http://www.thegreenbow.com/
Tiny	http://www.tinysoftware.com/
VirusMD	http://www.virusmd.com/
VisNetic	http://www.deerfield.com/
ZoneAlarm	http://www.zonelabs.com/

APPENDIX B – AVAILABLE HARDWARE FIREWALLS

The following is a list of hardware firewall manufacturers and their websites. It is by no means complete. Links to reviews of many of these products are available on <http://www.firewallguide.com/>.

2Wire	http://www.2wire.com/
Asante	http://www.asante.com/
D-Link	http://www.dlink.com/
Hawking	http://www.hawkingtech.com/
Linksys	http://www.linksys.com/
Macsense	http://www.xsense.com/
MultiTech	http://www.multitech.com/
Netgear	http://www.netgear.com/
Nexland	http://www.nexland.com/
SMC	http://www.smc.com/
Snapgear	http://www.snapgear.com/
SofaWare	http://www.s-box.com/
SonicWall	http://www.sonicwall.com/
WatchGuard	http://www.watchguard.com/
Zyxel	http://www.zyxel.com/

APPENDIX C – NETWORKED RESOURCES FOR HOME NETWORKING

We have found the following websites very useful for information about home networks and personal firewalls.

<http://www.firewallguide.com>

<http://www.homenethelp.com>

APPENDIX D –KNOWN BACKDOOR PORTS

A good list of known Trojan and backdoor ports can be found on the Simovits Consulting website (<http://www.simovits.com/>).

APPENDIX E – GLOSSARY

The following are definitions of computer related terms in this report. More computer related terms than you ever believed existed are available in *The Jargon File* (<http://www.tuxedo.org/~esr/jargon/>).

ACK Packet – A TCP/IP packet with the ACK (acknowledge) flag set. It is used to acknowledge the successful receipt of a packet.

Administrator – The highest level of access on a Windows system. Equivalent to root on a UNIX based system. The Administrator of a system can do anything on that system.

Adware – Software that displays ads on your computer and attempts to target the ads to your browsing habits. See also spyware.

Backdoor program – A hacker's version of pcAnywhere. That is, it allows a remote user to take control of a system, see what is on the desktop, capture keystrokes, move and click the mouse, and run any program on the system. Backdoor programs are distributed by viruses and worms and are sent to users via e-mail. The e-mail versions generally have a provocative title designed to get the user to run it. When a backdoor program is run once on a system, it installs and hides itself and makes settings that restart it whenever a system is rebooted. Some backdoor programs advertise their availability to specific sites or to IRC chat groups.

Blended Threat – Malicious code that is a combination of types. Blended threats combine the capabilities of viruses, worms, Trojans, and exploits to increase the likelihood that they can get to and take control of a system.

Broadband – High-speed, Internet access. In this paper it includes everything but dial-up modems. Most broadband connections are on all the time and includes, cable modems, DSL, and ISDN. ISDN is included here with Broadband connections even though it does require a dial-in.

Byte – A chunk of digital data consisting of eight binary bits. The amount of information needed to encode a single character.

Cable Modem – A modem for connecting a computer to a cable TV network and route digital data through that network. Cable networks currently operate at speeds of about 400k bits per second.

Command Shell – A text interface to an operating system. The shell is able to interpret and execute typed commands.

Daemon – A program that stays in memory and provides some service to other programs on a computer or to programs that connect to it through a network port.

Dynamic Host Configuration Protocol (DHCP) – A method of sharing IP addresses. When systems first connect to the network, they request an IP address from the DHCP server. The server returns the address along with other network configuration data.

Dial-up modem – A method of sending digital data using analog (voice) telephone lines at a rate of up to 56k bits per second. Digital data is converted into a series of tones that are sent over the analog lines and converted back into digital data by another modem at the other end.

Domain – A Windows networking term for all the machines that participate in a single grouping for networking and authentication services. Login credentials are stored on a Domain server and a user need login only once to get access to all the machines he is allowed access to within the domain.

Domain Administrator – The administrative account for domain level logins In a Windows Domain. Domain Administrators generally have administrative access to all the machines in the domain.

Domain Server – The main administrative server in a Windows domain. It stores the login credentials for all the machines and users in the Domain.

DoS – Denial of Service (note the lower case “o”). An attack where a server is overwhelmed in some way to prevent it from accepting connections from legitimate users. Bogus connection attempts are often used to overwhelm a system.

DoS Master – The controlling machine in a Denial of Service (DoS) attack. The Master machine controls multiple Zombies that perform the actual attack. See also Zombie.

DOS – Disk Operating System (note the upper case “O”). Microsoft’s older, pre-windows, command line operating system.

Drone – See Zombie.

DSL – Digital Subscriber Line. A high-speed data connection that uses telephone wires to send digital data at rates up to 1.5m bits per second. A user must be within 1.5 miles of the telephone substation.

Dumpster Diving – Digging through the trash to find usernames, passwords, and other information to use to compromise a system.

ESSID – The network name of a wireless network.

Exploit Scripts – See Scripts.

Exploits – See Scripts.

FAT, FAT16, FAT32 – File Allocation Table type of file system. This type of file system is used on DOS and the DOS based Windows systems (Windows 3.2, 95, 98, ME). It has no file access protections. The number refers to the size (bits) of the block descriptors in the file allocation table. The bigger the descriptors, the more blocks a drive can be broken up into. A block of sectors is the smallest chunk of a disk drive that can be allocated to a file. FAT (=FAT12) file systems had too few blocks for new, larger disk drives, hence the creation of FAT16 and FAT32. See also NTFS.

File Authorization – See Program Authorization.

File Transfer Protocol (FTP) – A protocol and program for transferring files between two computers via a network.

FIN Packet – A TCP/IP packet with the FIN (finished) flag set. Tells a remote system that no more data is coming. Used to close a properly opened session.

Firewall – A hardware or software device that controls access in and out of a subnet. Using a set of rules, a firewall examines (filters) every packet attempting to enter or leave a network and decides if the packet can continue or not.

FTP – See File Transfer Protocol.

Guest – An account on most systems that allows unauthenticated access to a system. This can be an extremely bad security hole if it is not carefully controlled.

Gui – Graphical user interface. A computer interface that uses a mouse, windows, and menus to control a computer. See also Command shell.

Hacker – A computer user who is extremely knowledgeable and interested in the details about how a computer system works. This term has been misused as a name for computer intruders who break into systems and perform malicious acts.

ICQ – Short for “I Seek You.” An instant messaging service owned by AOL.

Internet – An internet is a collection of interconnected networks. The Internet (capital I) refers to the international collection of public networks that grew out of the Arpanet.

Integrated Services Data Network – A high-speed data connection that uses telephone wires to send digital data at rates up to 64k bits per second. ISDN is a dialed network like analog phones but is digital end to end. It can be connected to the Internet or directly connected to a company’s internal network.

Intruder – A computer user who breaks into other people’s systems.

ISDN – See Integrated Services Digital Network.

ISP – Internet Service Provider. A person or company that provides a connection to the Internet.

LAN – Local Area Network. The network on the inside of a router or firewall. The local network where all your machines are. See also WAN.

LanMan – The old Windows network authentication protocol. This protocol is used by Windows 95, and 98. See also NTLM.

Local Compromise – A type of attack on a system where an intruder with a normal user's account on that system is able to get root access to that system.

Logic bombs – Programs that wait for some trigger (date, user action, etc.) and then destroy files on a computer.

Login session – All the packet traffic associated with a single login to a networked resource. Also called a session. Communications between two computers is done with packets that contain one or more characters of data. To start a session, the two computers exchange three packets. All packets following the three are data packets. A single packet closes the session. All of the data in the data packets combined together is the session.

Malware – Malicious software. Computer code that is specifically written to do destructive or inappropriate things. For example, damaging or compromising a computer and its files. Includes: viruses, worms, Trojans, logic bombs, and exploits.

Media Access Control (MAC) Address – The built-in hardware address of an Ethernet card.

Middleware – Software that resides between a server and your data files. For example, an indexing program that generates a web index or a search engine that is executed by a web server in response to a web page and that returns data via the web server to the user.

NAT – Network Address Translation. A method to reduce the need for more IP addresses by allowing one address to be shared among several machines. It is also used to block access to the sharing machines by allowing only outgoing connections from the sharing machines and blocking incoming connections.

Network connection – A connection between two computers that is shared among many computers. Whichever computer needs to communicate with another puts packets on the network addressed to the receiver. All computers on the network listen for packets addressed to them. This is in opposition to a point-to-point connection.

NTFS – NT File System. The file system introduced with Windows NT. This file system has intrinsic file access control. See also FAT.

NTLM and NTLM2 – The newer Windows network authentication protocols. These have much better security than the older LanMan protocol.

One-time password – A method for authenticating with a remote system that uses a password that works for only one login. To make a second login requires a new password.

Packet – The smallest chunk of digital data sent as a unit over a network. A packet may contain a single keystroke or several pages of text plus all the source, destination, and routing information needed to get the data to its intended recipient. Maximum packet sizes are normally around 1500 bytes.

Packet Filtering – A method of filtering packets based on the contents of the packet stream. Packet Filtering must also employ stateful packet inspection in order to be able to look at the contents of the whole stream and not just a single packet. This is different from a simple packet filter.

Password Cracking Program – A program for determining the value of encrypted passwords by encrypting a possible password and comparing that to the encrypted password it is trying to determine. Password cracking programs have access to whole dictionaries (including foreign) of encrypted passwords so if a password is a word in a dictionary, it can be easily cracked.

Point-to-Point connection – A connection between two computers that is not shared with other computers. It appears to be a single wire connecting the two systems. All information sent down the connection is assumed to only be directed to the system at the other end of the connection. A telephone call is a point-to-point connection. This is in opposition to a network connection.

Port – A connection between an application program and a network. Port numbers are used to connect a program running on one machine with the appropriate program running on another. A network packet contains routing information that includes both the address of the machine the packet is being sent to and the port number of the running program on that machine. The routing information also includes the source address and source port so the program that received a packet knows where to send any reply.

Port Forwarding – Mapping of a port on a server host inside a firewall to a port on the outside interface of the firewall so the service can be accessed by users outside of the firewall.

Program Authorization (File Authorization) – A filtering method where only specific files or programs on a computer are allowed to connect to the Internet. This is primarily used to block outgoing connections by viruses and worms.

PSTN – Public Switched Telephone Network. The phone company.

Rcp – Remote copy. A program for copying files between two machines.

Remote Compromise – A type of attack where an intruder somewhere on the Internet attacks and gets root access to a system. The intruder does not need any access to the system other than the network connection to be able to compromise it. That is, he does not need a user account on the system (Local Compromise) or to have physical access to the system.

Rlogin – Remote login. A program for connecting to another system and opening a command shell there.

Root Access – A term describing the highest level of access on a system. A person with root access (equivalent to Administrator on a Windows system) on a system can do anything on that system. What an intruder wants most.

Rsh – Remote shell. A program for connecting to another system and opening a command shell there.

RST Packet – A TCP/IP packet with the RST (reset) flag set. Tells a remote system to reset the connection. Its primary use is to reset a connection when the connection has not been setup correctly.

Runlevel – Unix based operating systems have different runlevels numbered from 0 through 6 which determine which services are running for a particular situation. When you change runlevels, the system starts up and shuts down different services. The following lists the most common use for the different runlevels.

Runlevel – Use

- 0 – Halt, turn off all services and shut down
- 1 – Single-user mode, used for maintenance
- 2 – Not used (user-definable)
- 3 – Full multi-user mode, command line interface
- 4 – Not used (user-definable)
- 5 – Full multi-user mode, with an X-windows user interface
- 6 – Reboot, turn off all services and restart the system

Scanning – A method of determining what ports are open on what machines by sending packets to those ports to see how they respond. Scanning programs usually scan many ports on a single machine or single ports on many machines.

Scripts – This term applies to all automated processes. Originally these were interpreted programs written in the command language of the system being used or in a common interpreted language like Perl. Current scripts can be fully compiled programs. Scripts that automate security compromises are also called exploit scripts or exploits.

Secure Shell (SSH) – A program for creating an encrypted connection between two machines. SSH opens a command shell (command line interface) on the remote machine that a user can use to run programs and transfer files on the remote machine. SSH is available in both commercial and public license versions.

Secure Sockets Layer (SSL) – A method of encrypting network sessions between two machines that resides at the socket layer. Applications that use this kind of encryption do not need to know how it works, they only need to use the appropriate network port or socket. It is mostly used by web servers (https connections) but can be used by other communication protocols.

Service – A program running on a system that provides data or an action to another program or system. Services generally listen to network ports, waiting for requests for the service they provide. A web server service provides web pages to remote clients.

Session – See Logon Session.

Shell – See Command Shell.

Simple Packet Filter – A packet filtering mechanism that filters single packets based only on the routing information in that packet. This is different from Packet filtering.

Sniffer – A program that puts your network interface into promiscuous mode so it can capture copies of all packets on the attached network. Sniffer programs thus “listen in” to communications between other systems.

Social Engineering – A method intruders and malicious codes use to get access to information and systems by fooling a human user of that system. For example, an intruder might pose as a computer repairman to talk a user out of a password.

Split Tunneling – A VPN setup option that routes packets destined for the VPN network through the VPN tunnel and packets destined for other destinations directly to the Internet. When split tunneling is disabled, all packets must pass through the VPN network including those destined for locations outside of the VPN network.

Spyware – Software that watches your browsing habits and sends that information to a marketing company’s server. See also adware.

SSH – See Secure Shell.

SSL – See Secure Sockets Layer.

Stateful Packet Inspection – A firewall filtering method that maintains the state of a session so it can allow those packets belonging to a session to pass while blocking those that do not. Stateful packet inspection is especially needed in situations where a protocol uses more than one data connection such as FTP.

SYN Packet – A TCP/IP packet with the SYN (synchronize) flag set. The first packet in a TCP/IP session, requesting a remote system to open a port and synchronize the packet sequence numbers.

TCP Stack – The software drivers that handle network connections and decode network packets. When a packet of information is received from a network, it is passed up the stack until the packet type matches the type of packet a layer knows how to handle. The layer then decodes the information and passes it up the stack for more decoding. Eventually the information reaches the application program that it was destined for.

Telephone Modem – A device for sending digital information over analog telephone lines with a maximum speed of around 33k bits per second.

Telnet – A protocol and program for remotely logging into a system and creating a command shell.

Trojan Horse – A malicious code that appears to be one thing while doing another. For example, the AIDS Trojan deleted the files on your hard disk while you read about AIDS. See also virus, worm.

Unicode – A text encryption scheme that uses two bytes instead of just one to encode a single character. Unicode is needed for character sets that have more than 256 characters (such as Asian characters), which is the maximum number of characters that can be encoded with a single byte.

Virtual Private Network (VPN) – A networking option that creates an encrypted pipe between a system and a remote subnet. The system is made to appear to be directly attached to that subnet and all network communications pass through the encrypted pipe to protect them from being intercepted.

Virus – A malicious code that travels from system to system by attaching itself to other programs and documents. See also Trojan Horse, worm.

VPN – See Virtual Private Network.

WAN – Wide Area Network. The network on the outside of a firewall or network that connects to the Internet. See also LAN.

Web client – A computer program for displaying web pages. Web pages are requested from a web server and displayed by a web client. Internet Explorer and Netscape Navigator are web clients.

Web server – A computer program that makes web pages available to others via a network. Web clients send page requests to a web server and the server returns the requested page. Netscape and Apache servers are web servers.

Windows Domain – See Domain.

Wired Equivalent Privacy (WEP) – An encryption method for protecting wireless communications. The original WEP specification contained flaws that allowed the encryption to be broken with little difficulty. New systems improve the security

by increasing the size of the encryption key to 128 bits or by using the new WEP2 standard.

Wireless Access Point – A router that routes between wireless and wired networks. That is, it has an Ethernet connection on one side and a wireless antenna on the other. Most home wireless access points include basic firewall features such as NAT.

Wireless LAN (WLAN) – A computer network that uses radio communications (and occasionally infra-red) for networking.

Worm – A malicious code that transports itself from system to system, usually through some security hole including social engineering.

Zombie – A computer used in a denial of service (DoS) attack. A DoS Master machine controls multiple zombies. The zombies send the packets that actually comprise the attack. See also DoS Master.

Department of Energy

CIAC

Computer Incident Advisory Capability

Technical Information Department Lawrence Livermore National Laboratory
University of California • Livermore, California 94551