NIST United States Department of Commerce
National Institute of Standards and Technology

SECURITY FOR TELECOMMUTING AND BROADBAND COMMUNICATIONS

Recommendations of the National Institute of Standards and Technology

D. Richard Kuhn
Sheila E. Frankel
Miles Tracy

Note to Readers

Acknowledgements

Contents

Figures

Executive Summary

One of the most important trends in information systems and networking is the rapid growth in telecommuting. As employees and organizations increasingly demand remote connectivity to corporate and government networks, the security of these remote end points becomes increasingly critical to the overall security of a network. Accompanying and contributing to this trend is the explosive growth in the popularity of broadband connections for home users. These developments complicate the process of securing organizational and home networks. This document simplifies this complicated process by providing recommendations on securing a variety of applications, protocols and networking architectures.

Home broadband architectures face a variety of threats that, while present on dial-up connections, are easier to exploit using the faster, always on qualities of broadband connections. The relatively short duration of most dial-up connection makes it more difficult for attackers to compromise home users dialed-up to the Internet. The advent of "always on" broadband connections provides attackers the speed and communications bandwidth necessary to compromise home computers and networks. Ironically, as governmental and corporate organizations have hardened their networks and become more sophisticated at protecting their computing resources, they have driven malicious entities to pursue other targets of opportunity. Home users with broadband connections are these new targets of opportunity both for their own computing resources and as an alternative method for attacking and gaining access to government and corporate networks.

There are a variety of actions that organizations and individuals can take to secure their telecommuting and home networking resources:

All home networks connected to the Internet via a broadband connection should have some firewall device installed. Personal software firewalls installed on each computer are useful and effective; but separate, dedicated, and relatively inexpensive hardware firewalls that connect between the broadband connection and the home user's computer or network can provide greater protection. We recommend serious consideration of using both personal and hardware firewall devices for high-speed connections. Operating both a software personal firewall and a separate device provides the opportunity to both screen out intruders and to identify any rogue software that attempts to transmit messages from the user's computer to an external system. See Section 3 for details.

Web browsers should be configured to limit vulnerability to intrusion. Web browsers also represent a threat of compromise and need some additional configuration beyond the default install. Browser plugins should be limited to only those required by the end user. Active code should be disabled or used only in conjunction with trusted sites. The browser should always be updated to the latest or most secure version. Privacy is always a concern with Web browsers and the two greatest threats to this privacy are the use of cookies and monitoring of Web browsing habits of users by third parties. There are a variety of ways of addressing cookies that range from disabling to selective removal using a variety of third-party applications. Internet proxies that encrypt all data protect home Web surfers from monitoring and allow them to use both the Web and e-mail anonymously. See Section 4 for details.

Operating system configuration options should be selected to increase security. The default configuration of most home operating systems is generally inadequate from a security standpoint. File and printer sharing should almost always be disabled. The operating system and major applications should be updated to the latest and most secure version or patch level. All home computers should have an anti-virus program installed and configured to scan all incoming files and e-mails. The anti-virus program needs to have its virus database updated on a regular basis. Another concern for many home users is the surreptitious installation of spyware by certain software applications. This spyware while usually not intended to be malicious, reports information on a user (generally without their knowledge) back to a third-party. This information could be general information about their system or specifics on their Web browsing habits. There are now a variety of programs available for detecting and removing this spyware. See Section 5 for details.

Selection of wireless and other home networking technologies should be in accordance with security goals. A variety of home networking technologies have become available for home users who wish to connect their home PCs together to share resources. Some of these technologies are the same as their office counterparts (e.g., Ethernet) and others are intended to specifically meet the needs of home users (e.g., phone- and power-line networking). While most of these technologies are secure, several represent a threat to security of both the home network and, sometimes, the office network. In particular, wireless networking has several vulnerabilities that should be carefully considered before any installation. See Section 6 for details.

Federal agencies should provide telecommuting users with guidance on selecting appropriate technologies, software, and tools that are consistent with the agency network and with agency security policies. Users have a wide variety of approaches to choose from in establishing an off-site office. Sophisticated technologies such as virtual private networks can provide a high level of security, but are more expensive and complex to implement than other solutions. Many users, particularly if they do not require interactive access to agency databases, can be afforded with an adequate degree of security at very low cost and with little additional software, easing burdens on both the user and system administrators at the central computing system. See Sections 7, 8, and 9 for details.

The benefits and risks of telecommuting are here to stay. Computing resources and access to office networks while on the road or working from home are just too valuable for most organizations or employees to give up. While there will always be risk associated with remote access to an organization's resources, most of these can be mitigated through careful planning and implementation. By the same token even though broadband connections generally represent a greater threat than dial-up connections, the threat can be reduced through careful configuration and the judicious use of the security tools and techniques discussed in this document.

1   Introduction

One of the fastest growing trends in the workplace today is the movement toward telecommuting, both for employees who work from home and those who carry notebook computers with them to work while on travel. Accompanying the growth of telecommuting is the rapidly rising popularity of broadband networks for home use. Employees who need extensive off-site access to office systems frequently find dial up access impractical. Broadband systems provide data transfer rates that may be 10 – 100 times as fast as dial-up access, making it possible for off-site employees to work with large documents, spreadsheets, and other business information as easily at home as at the office. But the storage of sensitive information on home systems often raises real security concerns. The features that make broadband networks useful for telecommuting also make them attractive targets for intruders.

Broadband users face a variety of security threats that depend on how their system is used. Almost all users face a risk that intruders can read, change, or delete files on their personal computers. Another concern for the average user is the potential for an intruder to hijack the user's computer, establishing a "backdoor" that can be activated anytime the machine is online, giving the intruder control over the user's machine. The best-known backdoor tool today is Back Orifice 2000 (BO2K), from the U.S. hacker group Cult of the Dead Cow. BO2K is available at Web sites all over the world and can be downloaded by anyone who has access to the Internet. SourceForge.net, a clearinghouse for open source software, shows over 1,440,000 downloads of BO2K as of November 2001. Only a fraction of those downloading BO2K are likely to use it maliciously, but its widespread distribution demonstrates that sophisticated hacking tools are readily available.

The most widely reported Internet security problems of the past few years are "denial of service" attacks against large commercial sites. In these attacks, intruders placed Trojan horse programs on computers operated by universities and other organizations that had persistent/high-speed Internet access and relatively little security. At a given signal, the attacker's Trojan horse programs to conduct a coordinated attack against other sites, sending messages at a rate too high for the sites to handle. With the explosive growth in broadband services, high speed Internet access for home users makes it likely that future denial of service attacks may use Trojan horse programs planted on home computers.

Until recently, consumer use of the Internet was generally limited to dial-up connections using a modem over telephone lines. Transmission speeds were typically limited to a range of 28K through 56K. With the advent of cable modems and digital subscriber lines (DSL) and other broadband connection options, connection speeds for home users have begun to approach those previously available only to large corporate and government subscribers.   High-speed connections bring a variety of benefits to home users – streaming video over the Internet, fast software downloads, interactive multiplayer games, and two-way video communications – but the new Internet technologies can also increase risks for home users.

In general, broadband connections supply the same services as dial-up connections to an Internet service provider (ISP): e-mail, Web browsing, online purchasing, and music and video access. The most obvious difference between dial-up connections and broadband connections is the latter's much higher transmission speed.   From an end-user perspective, broadband technologies differ in two fundamental ways from dial-up modems:

- "Always on" connectivity. One of broadband's greatest advantages, the relatively permanent nature of the connection, leaves a system exposed to potential intruders for much longer periods than dial-up. This makes it more likely for intruders to detect the system in a random scan, and provides a longer window of opportunity to compromise a system.

- High-speed access. Because broadband connections are so much faster than dial-up, intruders can download information from a system in seconds that otherwise might take long enough for the user to notice the activity. Similarly, intruders can upload viruses or other types of Trojan horse programs without the user detecting that the suspicious activity.   Malicious software loaded in this way may be used to steal private information from the user, to launch denial of service attacks, or to turn a user's machine into a pirated software ("warez") distribution server.

These features change the nature of the risks involved in Internet access, and require additional security measures not maintained by most users. Although the risks and safeguards are different for broadband connections, DSL and cable modem connections can be brought to a reasonable level of security with modest additional resources. This document explains the risks involved with broadband connections and outlines ways in which home users can protect their computing systems at reasonable cost and effort.

1.1   Document Purpose and Scope

This document is intended to assist those responsible – users, system administrators, and management – for telecommuting security, by providing introductory information about broadband communication security and policy, security of home office systems, and considerations for system administrators in the central office. It addresses concepts relating to the selection, deployment, and management of broadband communications for a telecommuting user. This document is not intended to provide a mandatory framework for telecommuting or home office broadband communication environments, but rather to present suggested approaches to the topic.

1.2   Audience and Assumptions

The intended audience for this document includes end-users, system administrators, and management personnel. Wherever possible, we have taken a "cookbook" approach, providing step-by-step instructions for configuring systems and selecting security options. This document is not technically detailed, however some sections assume background knowledge of TCP/IP (Transmission Control Protocol/Internet Protocol), the protocol suite used by the Internet, and various other aspects of networking and information security. Less-technical readers may find NIST Special Publication 800-10, *Keeping Your Site Comfortably Secure: An Introduction to Firewall Technology*[11] a useful starting point for network security topics and then go on to read this publication.

---

[1] Available at http://csrc.nist.gov

1.3 Document Organization

Section 2 introduces broadband communications technologies, and the security considerations associated with them. Section 3 discusses the use of personal firewalls, which are essential in protecting a home computer from intrusion. Sections 4 and 5 provide instructions on how to configure PCs and web browsers for added security. In Sections 6 and 7, advanced topics are introduced. Section 6 explains home networking, and how a home network can be protected. Section 7 describes virtual private networks, which are sophisticated technologies that can provide telecommuters with security approximating that available from an isolated inter-office network. Section 8 compares alternative approaches for securing e-mail and data transfer, depending on the user's needs and value of the data. Section 9 summarizes considerations for telecommuting security. Appendixes provide useful checklists, software update procedures, and additional resources available on the internet.

2   Overview of Broadband Communication

Although cable modem, DSL, and satellite systems deliver high-speed access to the Internet, they work differently, which affects security considerations. This section provides an overview of DSL, cable modem and satellite broadband network architectures.

2.1   Cable Modem Network Architecture

Cable television connections typically provide capacity for 110 channels of programming. For subscribers, some of this capacity will be unused. A cable modem takes advantage of the unused capacity to provide Internet access. One channel (usually in the 50 - 750 MHz range) is used for "downstream" traffic from the Internet to the home, while a second (normally 5 - 42 MHz) is allocated for "upstream" traffic from the user's computer to the Internet. Cable modems allow download speeds of up to 1.5Mbps. A cable modem converts data to and from the user's PC into signals on the cable line. At the cable provider facilities, a headend cable modem termination system (CMTS) connects the cable modems to the Internet, similar to an office local area network (LAN). A simplified diagram of this architecture is shown in Figure 1.

The cable modem system employs a "bus" approach where several cable modems that connect to a common point and share the available bandwidth between that point and the Internet. Generally, each cable modem on the system has an individual Internet Protocol (IP) address, which changes somewhat infrequently. Certain installations or services also use or provide semi-permanent static IP addresses.
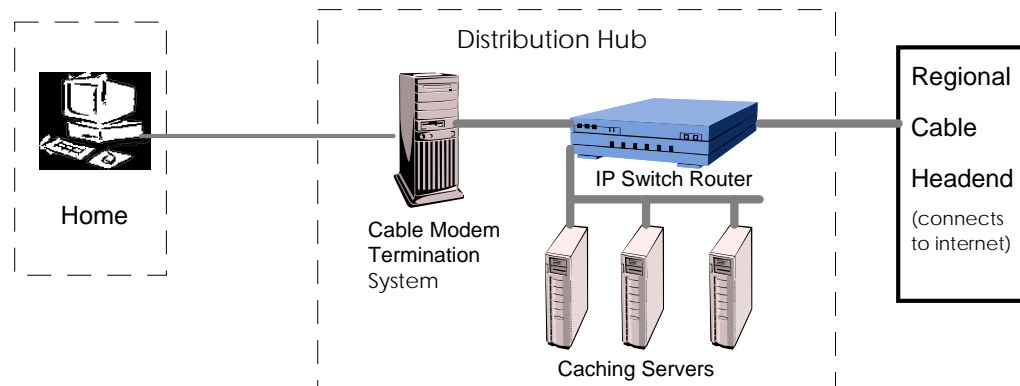
Figure 1 — Cable Modem Connections to Internet

2.2   DSL Network Architecture

DSL is another popular high-speed connection technology that works over ordinary telephone lines. A variety of DSL systems are available, but Asymmetric Digital Subscriber Line (ADSL) is most common for home use. With ADSL, frequencies below 4KHz are reserved for voice and the frequencies above that allocated for data. The telephone line can thus carry both voice and data simultaneously, and the PC can remain continuously connected to the Internet. Depending on the type of service, DSL download

speeds range from 256Kbps to 8Mbs, and 16 Kbps to 640Kbs bits for uploads. The bandwidth is relatively constant because connections do not share a common line unlike cable modems. Many DSL systems allocate IP addresses from a common pool each time the PC is rebooted or after a fixed period of time (dynamic IP addressing), but some DSL services now provide a semi-permanent IP address (static IP addressing), as a result of demand for online gaming and Web servers. Static IP addresses, since they do not change, are somewhat more risky than dynamic IP addresses. IP address that do not change regularly are easier for a hacker to attack and are more vulnerable once compromised, since the hacker can easily locate the compromised host in the future for further exploitation.

2.3   Satellite

Although less popular than either cable modems or DSL, satellite broadband is the only service that is available nearly nationwide. The system is a hybrid system that uses a regular phone line and modem for data and requests sent from the user's machine and uses a satellite link for send data to the users[2]. The uplink (modem) is, of course, restricted to the bandwidth the user can achieve with a regular modem (56 Kbps). The downlink (satellite) supports speeds up to 400 Kbps. Since it relies on a modem, satellite generally does not face the same threat as other broadband connection as it is not "always on." Figure 2 below illustrates an example satellite broadband connection. When a user attempts to access a Web page, the request is sent from the modem to the ISP. The ISP then forwards the request to the appropriate Web server. When the Web server receives the request, it processes the request. Instead of sending it back via the modem, it sends the Web page to the satellite provider's uplink station. The Web server does this because the user's request contains a special hidden "tag." The satellite uplink station broadcasts the data to the appropriate satellite, which rebroadcasts the data to the user's satellite receiver, which then forwards the data to the Web browser.

---

[2] As of this writing at least one satellite Internet service provider is in the process of upgrading their system so that all traffic will be sent and received via satellite.
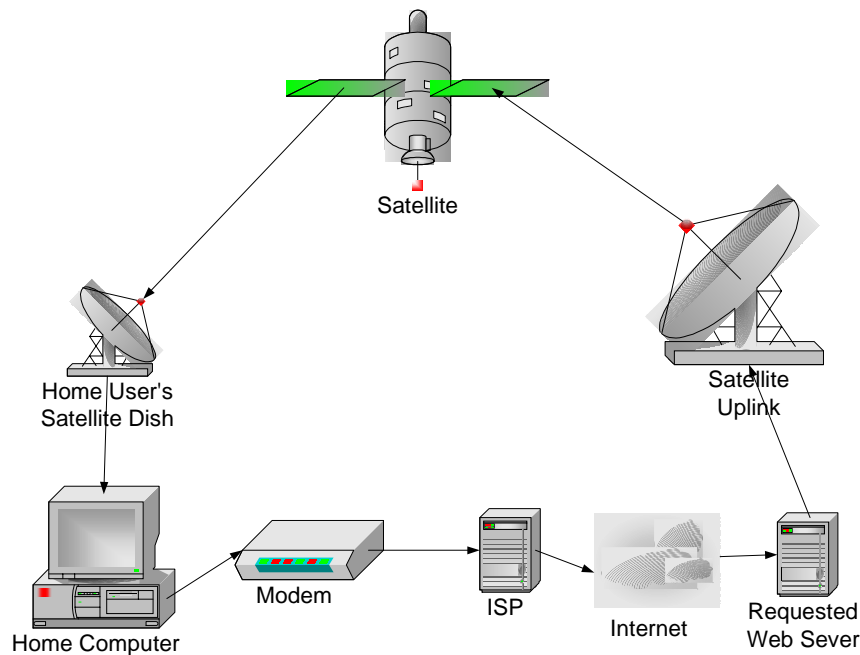
Figure 2 — Satellite Broadband Network Architecture

2.4   Risks of Broadband Connections

Whenever a computer is connected to the Internet, there is risk of unauthorized access. When using a dial-up connection, the risk is decreased because the duration of the connection is short for most users. With each logon, the user receives a different IP address. To penetrate a system connected via dial-up, an intruder would require the host's current IP address and would have to compromise the host in a relatively short period of time before it was disconnected.

With dedicated broadband connections, a computer is connected to the Internet—and capable of sending and receiving data — whenever it is on. If the computer is turned on in the morning and off in the evening, connection time may be 10 – 14 hours a day, which significantly increases the risk that the computer may be attacked. Even though a user may be using the machine only a few hours each day, the machine remains connected to the Internet, which greatly increases the window of opportunity for an attacker to compromise the computer.

Certain dedicated connections, particularly DSL lines, use dynamic IP addresses, similar to the way dial-up connections operate. While this may reduce the risk of an attacker targeting a *specific* user, it does not significantly reduce the risk to the average user. Most intruders arbitrarily scan the Internet for vulnerable systems. If a computer is powered on in the morning and powered off at night, the IP address will remain the same during the entire day. An attacker who finds the machine during a random scan may potentially have several hours to penetrate the system.

While many users are aware of the risks associate with using the Internet, relatively few have a sense of the magnitude of risk. Figure 3 shows a log of intrusion attempts recorded over a 10-day period on a machine connected by cable modem running 24 hours a day. The log was generated by a firewall configured to a high security level, and most of the apparent attempts were judged to be false alarms. However, potentially serious intrusion attempts were recorded at a rate of more than three per day.
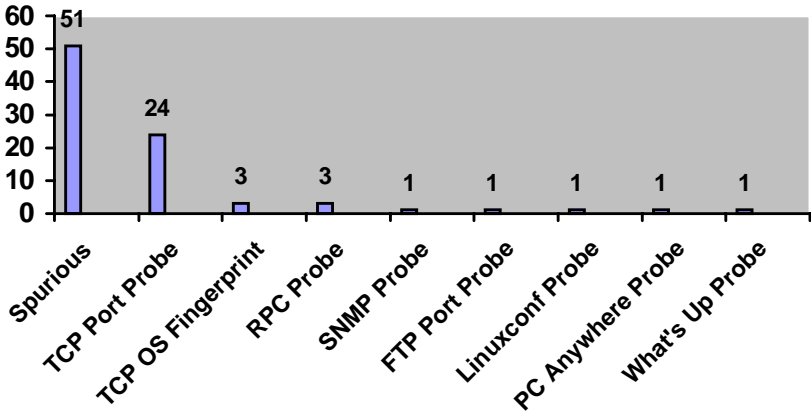
Figure 3 — 10-Day Record of Intrusion Attempts

"Probing" is the first step an attacker takes when identifying vulnerable systems. Probing is the hacker equivalent to "rattling door knobs" looking for unlocked doors. Probes attempt to determine if a computer will respond to particular kinds of messages. This "banner grabbing" process can also help an attacker identify various services or server programs that a system is running so that the attacker can exploit known vulnerabilities. More serious probes are "fingerprint" efforts, which attempt to determine what operating system is running on a particular computer by analyzing the pattern of communication services listening. The intrusion attempts depicted in Figure 3 occurred on a machine with a cable modem connection, so nearly all are the result of probes against random IP addresses. Although none of the attacks were successful, this example demonstrates that security is most critical with broadband connections. If you operate a computer connected to the internet, you will be scanned.

3   Personal Firewalls

The first line of defense for the home broadband user is a good network firewall. Although most users are aware of highly publicized Internet break-ins and denial of service attacks, few have evaluated their own system's vulnerability to such attacks. Those who have are often surprised to learn that their PCs have significant weaknesses. One online scanning service (www.DSLreports.com)[3] found that more than 95 percent of the machines scanned have one or more possible vulnerabilities. Typical problems included public machine names or user names, guest accounts, routers with weak configuration protection, and printers visible for anyone to use.

Table 1 — Manufacturers of Software Personal Firewalls

Personal Firewall Product	Web Site	Cost	Platform
BlackIce	www.networkice.com	yes	Windows
McAfee Personal Firewall	www.mcafee.com	yes	Windows
NeoWatch Personal Firewall	www.neoworx.com	yes	Windows
Norton Personal Firewall	www.symantec.com	yes	Windows
PC Viper	www.pcviper.com	yes	Windows
Securepoint	www.securepoint.cc	Free	Windows
Sygate Personal Firewall	www.sygate.com	Free[4]	Windows
Tiny Firewall	www.tinysoftware.com	Free[5]	Windows
Winproxy	www.winproxy.com	yes	Windows
ZoneAlarm	www.zonelabs.com	Free/ yes	Windows
SmoothWall	www.smoothwall.org	Free	Linux
T.Rex	www.opensourcefirewall.com	Free	Linux
SINUS	www.ifi.unizh.ch/ikm/SINUS	Free	Linux
Net Barrier	www.intego.com/netbarrier	yes	Mac OS

For years, large organizations have operated firewalls to reduce the risk of unauthorized access to their networks. A firewall is simply a filter that allows certain types of packets, or message fragments, to enter and exit a network, while rejecting others. Network firewalls can have complex rule sets that determine which packets are accepted and which are rejected. Corporate firewalls can be costly to configure and operate. The advent of broadband access for home users has established a market for firewalls for home use. In most cases these "personal firewalls" are software add-ins that filter packets going to and from the cable modem or DSL connection. Several are available free to home users and others are relatively inexpensive, typically below $40 (see Table 1[3]). Personal firewalls

---

[3] Certain commercial products are described in this document as examples only. Inclusion or exclusion of any product does not imply endorsement or non-endorsement by NIST or any agency of the U.S. Government. Inclusion of a product name does not imply that the product is the best or only product suitable for the specified purpose.

[4] Free for personal use only.

[5] Free for personal use only. Cost for business use.

are designed to be easy to install and operate, and can significantly reduce the risk of intrusion.

In addition to the personal firewall software installed directly on your computer there are dedicated hardware-based personal firewall/router devices. These devices are installed between the cable/DSL modem and your computer(s). See Figure 4 for an example home network employing a hardware-based firewall.
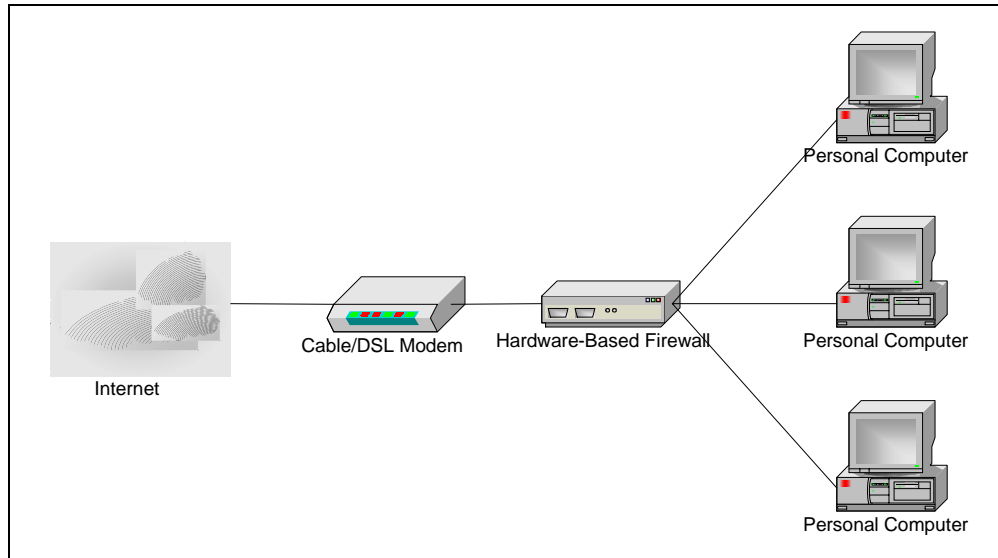
Figure 4 — Hardware Firewall Network Diagram

Although these generally cost more ($75.00-$200) they offer several advantages over the software firewalls. Perhaps most important is that they allow several computers to share the same cable/DSL modem without an additional charge from the service provider (check service agreement to determine if this is permitted by the ISP). This is accomplished through network address translation (NAT). NAT translates your external public IP (assigned by your ISP) into multiple internal private IPs. This allows each computer system to be on an internal network with a private IP address space that is not accessible from outside of the network. This increases security, as all connections from the internal network to the Internet must be initiated from an internal system. The NAT capabilities within the router translate the internal private addresses to the external public IP. This allows all internal systems to share one external IP while adding another layer of protection. When combined with the firewall capabilities inside the router, access to each individual computer can be controlled while preventing outside access. Unauthorized and un-initiated traffic from outside the router is not allowed while traffic from inside can either be allowed or denied depending on the firewall rule settings. In addition, due to their specialized design, dedicated hardware firewall implementations are generally more difficult to compromise than software that depends on an underlying operating system for security.

With hardware firewalls, it is critical that all default passwords are changed immediately to stronger passwords. If this is not done, anyone that knows these default passwords can have complete control over your firewall. Lists of manufacturer-assigned default passwords are widely available on the Internet. In addition to this, many router/firewall combinations come pre-configured with machine firmware. Firmware is analogous to an operating system for a desktop computer, dictating how the device will operate, including

firewall functionality. Often, hardware firmware contains memory space to store passwords for administering the device. Because manufacturers publish updates to their machine firmware to mitigate security vulnerabilities, it also critical to check the manufacturer website for firmware updates and apply them.

3.1   Firewall Features

Not all personal firewall products have the same set of features and options. A number do not provide all the features discussed below. Users should review products carefully.

Logging: Ensure that logging is enabled on the firewall. If an intruder breaks into your machine, the log may help to identify the source of the intrusion. In addition, cooperative efforts have been organized to collect log information to help identify attackers who scan thousands of IP addresses. System administrators can forward logs to a collection site that combines the information with other logs, making it possible to track and potentially identify attackers that have scanned IP addresses.

Port hiding or "stealth" mode: Computers receive packets directed to specific port numbers, each allocated to a specific service such as Web servers or remote file access. When a packet is received, the service sends back a reply packet to establish the connection. A firewall ignores selected ports, effectively hiding the existence of that port. Most firewall products require no special user knowledge to configure ports that should be hidden.

Automatic lockout: One of the most significant security problems with broadband connections is their "always on" nature. Certain firewall products allow users to set a timer that will stop all Internet access to and/or from the machine after a specified length of inactivity. When the user resumes activity, the Internet connection is restored. This feature greatly reduces the amount of time that a machine is accessible to intruders, since a connection exists only when the user is active on the machine.

Connection notification: A number of firewalls can be configured to notify users when a particular program requests access to the Internet. When a program initially attempts to send out packets, the firewall will interrupt the user with a message such as "Should [program name] be permitted to connect to the Internet?" The user can then answer "yes", usually with an option to not require confirmation for the same program again, or "no", to provide time to investigate further. This feature sometimes identifies the existence of "spyware" or backdoor programs that may have been installed without the user's knowledge.

"Paranoia level" tuning: If a firewall is configured for a high level of security the potential for false alarms increases. Most firewalls allow users to set a level of security that is appropriate for the intended use. For example, if users are operating a file-sharing program, particular packets may trigger the firewall unnecessarily. A more moderate level may reduce false alarms while providing security that the user considers appropriate. The appropriate security level for an end-user may not necessarily be apparent as soon as the firewall is installed or configured. For this reason manufacturers make changing the security level a simple task to accomplish.

Configurable rule set: Certain firewalls are designed to operate under a rule set determining access control. Often times this rule set will examine all packets both inbound

and outbound for their protocol specific properties such as: port, type of service (FTP, HTTP, SMTP, etc.), destination/source IP address, etc. Firewall rule sets are designed to limit these values at the user's discretion. This rule set can be extended with custom rules that match an individual's needs. Adding rules or changing existing ones does require some degree of networking experience and should only be performed by qualified personnel.

Password protected configuration: Certain firewalls offer the ability to assign a password to the settings you define during configuration. This password may then be prompted for each time another user wishes to make a configuration change to your firewall. This protects your firewall and network from an inside user with bad intent.

3.2   Establishing a Secure Firewall Configuration

Establishing a security firewall configuration depends of the type of firewall a user has implemented, either software or hardware-based. To establish a secure configuration of software-based firewall, set the firewall to the highest level of security and decrease it as needed. You should be aware that improper configuration of your firewall, or too restrictive of a security setting can prevent all types of network access both inbound and outbound. Although not all of the steps described below can be performed on all software-based firewalls, at a minimum, the most secure setting for a software-based firewall should do the following:

- **Log the IP address and date/time of possible infractions**.

   This functionality is implemented by default for virtually every major firewall available, and in many cases this information is found in the firewall log. You should still examine the log settings on your firewall, and the contents of the log file itself to familiarize yourself with it. Those users operating on broadband Internet connections should be aware of the possibility of a high number of false positives from their firewall. What this means is that just because a firewall may alert that your computer was just scanned for infection of a common Trojan horse, this does not mean you are actually infected. Depending on the connection attempt being made, your firewall may have interpreted certain packets incorrectly, or your computer may be one in a block of hundreds of IP addresses just scanned for possible infection.

- **Drop all incoming packets to known insecure services (e.g. TCP/UDP ports 135 to 139 which support NetBIOS protocol)**

   You have the ability to restrict access to arbitrary ports during the configuration of your firewall. While restricted, the firewall is causing these ports to operate in stealth mode, not responding to connection attempts, behaving as if the computer were turned off. Many host-based security scanners will list stealthed/blocked ports as closed when scanning a system with a personal firewall. Lists of insecure ports are widely available on the Internet.

- **Drop all outgoing packets, except for the services that are allowed (e.g., DNS, SMTP/POP/IMAP, HTTP, FTP, etc.)**

   Although this ability is implemented in many different ways depending on firewall vendor, the underlying concept is that all network activity originating from your machine, or destined for it, should be dropped or ignored immediately unless you

11

have explicitly allowed it in your configuration. Certain firewalls are configured to automatically look for and prevent activity that matches communication from well-known Trojan horses. These settings should not be disabled unless you are aware of the ramifications.

- **Enable stealth mode**

  Certain firewalls have the ability to enable "stealth" mode on both a specific port level and a system wide level. When operating in stealth mode on a system wide level, the firewall forces your computer not to respond to requests from network discovery tools such as ping and port scanners. Even though your computer does not respond to these tools, you can still access network services such as email and web sites in a normal fashion.

- **Shutdown system's Internet connection when it is not in use**

  Although you can operate proactively to enhance the security of your systems in many ways, assuming that there is no such thing as "perfect security" goes a long way towards the safety of your systems and personal data in the long run. Because of this, preventing all access to the Internet when your computer is not in use ensures that rogue services cannot operate when you are not around to catch them. This feature is often very easy to implement on firewalls forcing you to toggle a "lock" between open and shut.

- **Enable connection notification.**

  Firewalls that are built with connection notification can alert you to every single service that is attempting to access the network on your computer. As stated previously, this can possibly help to detect the presence of a Trojan horse service. If you interact with a computer long enough, you begin to create a functional baseline of in your mind of the normal operation of your system. If an alert appears for a service that you are not familiar with, you should investigate this further, search for this service on your hard drive, determine if it should be there or not and consult support services if you are unsure of what to do.

Because hardware-based firewalls often offer functionality that is not found on software-based firewalls, establishing a secure configuration follows a slightly different process. You should be aware that many hardware-based firewalls ship with all security settings disabled out of the box.

- **Change default administration password**

  As discussed earlier, those devices that offer configurable settings are set with a default password. The first task in configuring your hardware-based firewall is changing the default password.

- **Check for hardware firmware updates**

  Hardware-based firewalls use a firmware to configure and store its settings. This firmware is often stored in programmable read only memory (PROM) or flash memory. Similar to software updates for your desktop computer, manufacturers publish updates to firmware when security vulnerabilities or defects are

discovered. Develop a habit out of checking for and applying possible firmware updates to your hardware-based firewall on at least a monthly basis.

- **Disable WAN requests/enable stealth mode**

  Many hardware-based firewalls are designed to not respond to WAN requests. WAN requests include traffic generate from network discovery tools such as ping or port scanners. Enabling this setting causes the device to behave in a stealth mode essentially rendering your entire network invisible to the outside world.

- **Block all unnecessary public/DMZ machines**

  Many hardware-based firewalls offer some type of publicly visible machine/DMZ machine option.   Be very careful about enabling this option for any machine(s) on your network because this causes them to be accessible by the outside world. Disable all public machines unless explicitly necessary.

- **Ensure all unnecessary ports are closed (port forwarding)**

  As an alternative to, or in tandem with a DMZ option, many hardware-based firewalls allow port forwarding. This is a situation where only a specific port may be visible to the outside world. If you are implementing port-forwarding, only open those ports that are explicitly needed. Any other publicly visible port should be considered a security risk.

- **Restrict or disable remote administration from a WAN interface**

  Remote administration is rarely necessary for a home system, since the user will normally have daily access to the system.   Disabling remote administration prevents intruders from taking control of a firewall across the internet.

3.3   Running an Online Security Assessment

There are numerous free Web sites that will "scan" your home PC and provide a report of its network security posture.   When these sites scan your machine, they attempt to connect to various services (sometimes referred to as ports) that are running on your machine. If the scanner finds an operational service, it will attempt to gather additional information from that service (e.g. version, operating system identification, etc.).   The information gathered in this enumeration phase will then be compared to a database of known vulnerabilities and the site will then provide a score or rating of your computer's network security posture.

To have one of these sites scan your home PC or network, you will need to visit their Web site and request a test. Generally, the results are provided in real-time via an encrypted Web page as the scan is performed. There are two types of tests performed by these sites. The most basic is a "port scan" that reports what services or applications are available from the Internet. A port scan helps to quickly identify possible problems, but it makes no attempt to identify the vulnerabilities associated with the identified services. Therefore, most users should also run a vulnerability scan. While there is very limited risk associated with these tests, it is recommend that users close all applications and save

data to the hard disk prior to starting the test. Table 2[6] provides a comparison of several popular online security assessment Web sites. Note that some of these sites scan different sets of ports; it is advisable to run scans using more than one assessment site. After running the scan, print or save the results, then consult the agency system administrator about how to resolve any potential security issues raised by the scan.

Table 2 — Online Security Assessment Web sites

Service	URL	Port Scan	Vulnerability Scan
DSL Reports	http://www.dslreports.com/tools	✓	✓
GRC	http://grc.com/		✓
HackerWhacker	http://whacker2.hackerwhacker.com/	✓	✓
Microsoft Personal Security Advisor[7]	http://www.microsoft.com/technet/mpsa/		✓
Sygate	http://www.sygatetech.com/	✓	
Symantec	http://www.symantec.com/securitycheck/		✓

3.4 Summary Recommendations

All home networks connected to the Internet via a broadband connection should have some firewall device installed. Personal software firewalls installed on each computer give some protection but separate, dedicated hardware firewalls that connect between the broadband connection and the home user's computer or network can provide greater protection. Operating both a software personal firewall and a separate device provides the opportunity to both screen out intruders and to identify any rogue software that attempts to transmit messages from the user's computer to an external system.

---

[6] Certain commercial products are described in this document as examples only. Inclusion or exclusion of any product does not imply endorsement or non-endorsement by NIST or any agency of the U.S. Government. Inclusion of a product name does not imply that the product is the best or only product suitable for the specified purpose.

[7] Microsoft Personal Security Advisor (MPSA) only supports Microsoft Windows NT Workstation and Microsoft Windows 2000 Professional. For more information and instruction in using MPSA see Appendix B.

4   Securing Web Browsers

Browser security considerations discussed in this section apply to dial-up and broadband connections, but concerns may be more acute with broadband because of the higher speed connection. Not every user will require all of the browser features described below, but users need to be aware of the security concerns with each because they are increasingly used on Web sites. Each browser feature discussion is accompanied by both precautions for using the feature with less risk, and by procedures for disabling the feature if a user considers it a significant risk.

4.1   Browser Plugins

A browser plugin is a software application that handles a particular type of file on the Internet. Popular examples include plugins for video, such as Microsoft Media or Real, and electronic publishing applications such as Adobe Acrobat for displaying documents online[8]. Although these examples are used in thousands of Web sites, it is common for users to download a plugin for an interesting Web site, but never use that plugin again for months because the content type is unusual. This situation is likely to occur in newer application types where standards have not yet developed. For example, a user may download a 3D image plugin to view a particular Web site, but never encounter that particular 3D image type on other sites.

Normally, a particular type of content automatically triggers the associated plugin. That means that every plugin is an additional potential source of attack. A number of plugins have been shown to have extremely serious security vulnerabilities. For example, the Microsoft Office plugin in Internet Explorer 3 and 4 can be exploited allowing an attacker to run arbitrary code on the client machine.[9]

4.1.1   Precautions for using plugins

- Restrict plugin use to only essentials. For example, users may need to access document files using Adobe Acrobat or a Postscript viewer, but may not need other plugins.

- If possible, turn off potentially dangerous options on plugins that are not in use. For example, some Postscript viewers make it possible to disable Postscript's ability to modify arbitrary files when a document is viewed or printed.

---

[8] Certain commercial products are described in this document as examples only. Inclusion or exclusion of any product does not imply endorsement or non-endorsement by NIST or any agency of the U.S. Government. Inclusion of a product name does not imply that the product is the best or only product suitable for the specified purpose.

[9] See www.cve.mitre.org   Vulnerability ID: CVE-2000-0765. "Buffer overflow in the HTML interpreter in Microsoft Office 2000 allows an   attacker to execute arbitrary commands via a long embedded object tag, aka the "Microsoft Office HTML Object Tag" vulnerability."

4.1.2 Reviewing and disabling plugins on Netscape

1. To review plugins that are installed on your machine enter the Uniform Resource Locator (URL): "about:plugins" in the location bar. (This works even if the machine is not online at the time.)
2. From the menu bar select "Edit" then "Preferences."
3. Select the "Applications" item from the tree at the left.
4. A scroll list of various document types will appear on the right. (See Figure 5).
5. To remove a particular Plugin select it and press the "Remove" button. If you are unsure if it can be removed, you can click the "Edit" button and check "Ask me before opening downloaded files of this type" to tell Netscape to inform you whenever it would run this particular plugin. This will allow you to prevent a plugin from running if it seems inappropriate. For example, if the Web page you are viewing does not appear to have any spreadsheet content but a spreadsheet plugin is triggered, there may be an attempt to exploit a security hole in the plugin.
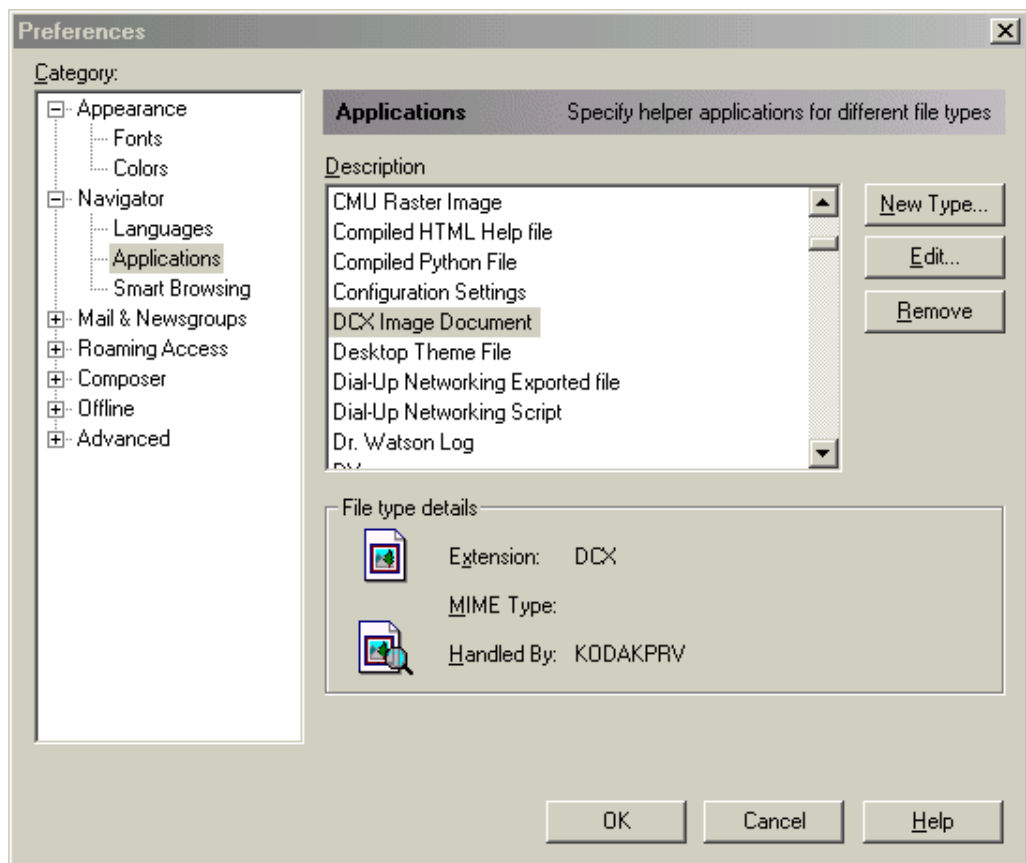
Figure 5 — Netscape Plugins

4.1.3 Reviewing and disabling plugins on Internet Explorer

Internet Explorer's settings for plugins are linked with the settings for ActiveX (see next section). The changes you make for plugins with affect ActiveX setting as well.

1. Open Internet Explorer.

2.   From the Internet Explore menu bar select "Tools" and then "Internet Options."
3.   The "Internet Options" window will open. From this window select the "Security" tab.
4.   Select "Internet", by clicking on the picture of a globe. (See Figure).
5.   Once Internet has been selected, click on the "Custom Level" button.
6.   This will open the "Security Settings" Window.
7.   From this window scroll down until you see the "Active-X and Plug-ins" section. There may be five or so different sub-sections in which you should select "Disable" in order to completely turn off all ActiveX components.
8.   Click the "OK" button at the bottom of the "Security Settings" window.
9.   Click the "OK" button at the bottom of the "Internet Options" window.
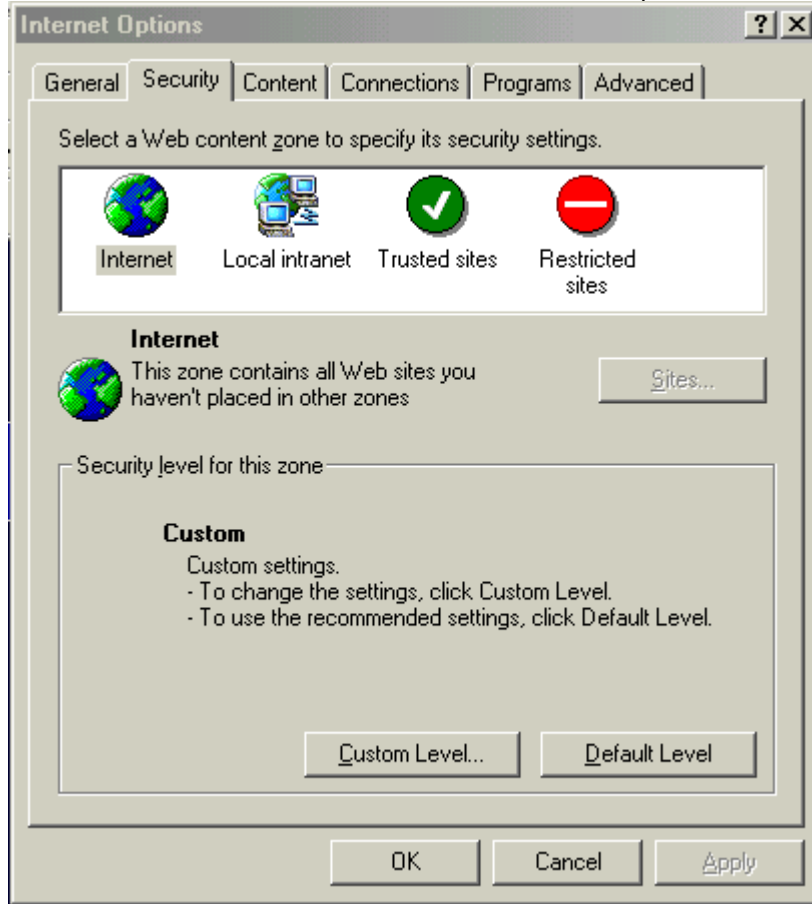
Figure 6 — Internet Explorer Plugins

4.2   ActiveX

ActiveX[10] is a powerful and useful technology from Microsoft that allows software applets (mini-applications) to be reused in a variety of applications (think of an Erector set or Lego

---

[10] Certain commercial products are described in this document as examples only. Inclusion or exclusion of any product does not imply endorsement or non-endorsement by NIST or any agency of the U.S. Government. Inclusion of a product name does not imply that the product is the best or only product suitable for the specified purpose.

blocks). Internet Explorer comes bundled with ActiveX support; Netscape requires a separate (nonstandard) plugin. The ActiveX security model places no restrictions on what applications can do; applications are simply signed by their developers using a signature scheme called Authenticode. Security thus depends on the trustworthiness of the developer, and the user's willingness to trust Web sites accessed employing ActiveX.[11]

ActiveX digital signatures are verified using identity certificates issued by a trusted third party certificate authority to an ActiveX software publisher. For an ActiveX publisher's certificate to be granted, the software publisher must pledge that no harmful code will be knowingly distributed under this scheme. The Authenticode process ensures that ActiveX applets cannot be distributed anonymously and that tampering with the controls can be detected. This certification process, however, does not ensure that an applet will be free of software errors. The ActiveX security model leaves the responsibility for the computer system's security to the user's best judgment. This is theoretically sound when all users are security experts but unrealistic in the real world.

Before the browser downloads an unsigned ActiveX control, or a control whose corresponding publisher's certificate was issued by an unknown certifying authority, the browser presents a dialog box warning the user that this action may be unsafe. The user can choose to abort or continue the transfer based on their best judgment. Unfortunately, users may be unaware of the security implications of the decision, which may have serious repercussions. Even when the user is well informed, attackers may trick the user into approving the transfer. In the past, attackers have exploited implementation flaws to cover the user dialogue window with another that displays an unobtrusive message, such as "Do you want to continue?" while exposing the positive indication button needed to launch active content. Hackers have also been successful at forging certificates in order to distribute malicious code.

4.2.1   Precautions for Using ActiveX

Because ActiveX is becoming more widely used, and is required for certain applications, it may not be practical to avoid ActiveX. If it is used, certain basic precautions should be followed:

- Ensure that Web sites viewed using ActiveX are operated by trusted organizations.

- Use the built in ActiveX security features.

- Only download ActiveX controls that have been digitally signed by a reputable software developer or publisher.

4.2.2   Disabling ActiveX

Although ActiveX employs digital signatures to verify the source of the component, it takes a moderately sophisticated user to investigate the source of the component and the

---

[11] This discussion is derived from NIST SP 800-28 Guidelines on Active Content and Mobile Code, October 2001, which may be consulted for more on Active X.

source of the Web page that is applying the component. As a result, certain organizations prefer to disable ActiveX rather than have their users take responsibility for determining the security of ActiveX applets. (Note: ActiveX controls are not natively supported on Netscape Communicator. This section applies only to Internet Explorer.)

From the menu bar select "Tools" and then "Internet Options." A dialog window will appear. From this window, select the "Security" tab.

1. Open Internet Explorer.
2. From the Internet Explore menu bar select "Tools" and then "Internet Options."
3. The "Internet Options" window will open. From this window select the "Security" tab.
4. Select "Internet", by clicking on the picture of a globe.
5. Once Internet has been selected, click on the "Custom Level" button.
6. This will open the "Security Settings" Window.
7. From this window scroll down until you see the "Active-X and Plug-ins" section. There may be five or so different sub-sections in which you should select "Disable" in order to completely turn off all ActiveX components.
8. Click the "OK" button at the bottom of the "Security Settings" window.
9. Click the "OK" button at the bottom of the "Internet Options" window.

4.3   JavaScript

Scripting languages, such as JavaScript, have been a source of security vulnerabilities in Web browsers. (Despite the similarity in name, JavaScript is completely different from Java, and does not contain the same security features as Java.) Many browser-based attacks stem from the use of a scripting language in combination with some other security vulnerability. For example, attacks that let Web sites steal files from client machines typically result from an interaction between JavaScript's ability to automatically submit forms and a programming error in the way form fields are initialized. A variety of attacks have been reported where JavaScript is used to mimic a trusted site. However, a large number of legitimate sites depend on JavaScript. Disabling it may render these sites completely unusable.

4.3.1   Precautions for using JavaScript

JavaScript is used extensively on the Internet, but most Web sites can be used (with some degradation in functionality) without it. No solutions have been developed for increasing the security of JavaScript. However, it is relatively low risk when browsing reputable sites. Users concerned with JavaScript security may wish to disable it when browsing sites that may not be trustworthy (see procedure below).

4.3.2   Disabling JavaScript in Netscape:

1. Open Netscape.
2. From the menu bar select "Edit" and then Preferences."
3. The "Preferences" window will open.
4. From left side of the "Preferences" window, select the "Advanced" category.
5. Deselect the checkbox labeled "Enable JavaScript."
6. Click the "OK" button at the bottom of the dialog window.

4.3.3 Disabling JavaScript in Internet Explorer

1. Open Internet Explorer.
2. From the Internet Explore menu bar select "Tools" and then "Internet Options."
3. The "Internet Options" window will open. From this window select the "Security" tab.
4. Select "Internet", by clicking on the picture of a globe.
5. Once Internet has been selected, click on the "Custom Level" button.
6. This will open the "Security Settings" Window.
7. From this Window, scroll down until you see the "Scripting" section.
8. Directly below this there will be a "Active Scripting" subsection.
9. Select "Disable" from the subsection.
10. Click "OK" at the bottom of " Security Settings" window.
11. Click the "OK" button at the bottom of the "Internet Options" window.

4.4 Java Applets

Java applets are programs written in Java programming language[12] that can be run in Web browsers. Applets might be used to add graphical drawings to a Web page or to act as a user interface to server-side programs. Java has a large number of built-in security features that are intended to prevent attacks, and has typically been one of the stronger links in the chain of Web browser security products. Nevertheless, several Java-based attacks have been conducted on various platforms, and disabling Java is an option that the security-conscious user may consider after performing other security safeguards.

4.4.1 Precautions for using Java applets

When Java is enabled on Windows or Unix, ensure that the environment variable CLASSPATH is not set when the browser is launched. This variable refers to directories containing trusted Java classes that are, on most browsers, executed with relaxed security restrictions

4.4.2 Disabling Java Applets in Netscape

1. Open Netscape.
2. From the menu bar select "Edit" and then Preferences."
3. The "Preferences" window will open.
4. From left side of the "Preferences" window, select the "Advanced" category.
5. Deselect the checkbox labeled "Enable Java."
6. Click the "OK" button at the bottom of the dialog window.

4.4.3 Disabling Java Applets in Internet Explorer

1. Open Internet Explorer.
2. From the Internet Explore menu bar select "Tools" and then "Internet Options."
3. The "Internet Options" window will open. From this window select the "Security" tab.
4. Select "Internet", by clicking on the picture of a globe.
5. Once Internet has been selected, click on the "Custom Level" button.
6. This will open the "Security Settings" Window.
7. From this Window, scroll down until you see the "Microsoft VM", or depending on the version of Explorer, "Java", section.

---

[12] Although named similarly, Java and JavaScript are two unrelated technologies. They were originally given similar names for marketing purposes.

8. Select "Disable Java."
9. Click "OK" at the bottom of " Security Settings" window.
10. Click the "OK" button at the bottom of the "Internet Options" window.

4.5   Cookies

Probably no aspect of Web browsers is better known – or more widely misunderstood – than cookies. Many Web sites offer users the option of "remembering" their password or retaining information used in greeting the user for later logins. This is accomplished using cookies, small files that let a Web server record some information on the user's PC hard disk[13]. This information (such as user ID and password) is then transmitted to the Web server every time the browser requests a page from that site. This lets the site "remember" what the user did on the site previously, and lets the site associate that information with the user when they return in the future. This is a convenient feature in many contexts: a cookie can be used to automatically display weather for a user's location, or remember a password or credit card number. If not handled carefully by the Web sites that use them, cookies can create a significant privacy risk. For example:

■   Cookie data is not encrypted and, therefore, one with access to your hard disk can view your cookie data. This is a problem if poorly designed sites use cookies to store sensitive data, rather than using an innocuous user ID which is only associated with real data on the server.

■   Although most reputable e-commerce companies have explicit privacy statements, companies can share or exchange cookie information without a user's knowledge. This sharing can give a third party indirect access to personal information.

■   By loading images from a mutual third party, two different sites can share cookies. This could let one site gain information about what you did at a different site. Netscape has a setting that still allows most cookies but prevents this problem (see below), but Internet Explorer does not.

4.5.1   Precautions for using cookies

Relatively few options are available for cookie management using the browser configuration settings. Some basic precautions follow:

•   Users concerned about privacy should consider disabling cookies for general Web browsing and temporarily enabling them only when necessary (for example for an online reservation service). After completion of the service that requires cookies, turn off the cookie option and delete cookie files (see information below for how to do this).

•   Netscape users can select the checkbox "Accept only cookies that get sent back to the originating server" under "advanced" preferences (see procedures below). This will reduce "profiling" cookies, which reduces privacy concerns.

---

[13] In essence cookies are used to add state to the stateless HTTP (web) protocol.

4.5.2   Disabling cookies in Netscape

1. Open Netscape.
2. From the menu bar select "Edit" and then Preferences."
3. The "Preferences" window will open.
4. From left side of the "Preferences" window, select the "Advanced" category.
5. Select the checkbox labeled checkbox "Accept only cookies that get sent back to the originating server" or, on earlier versions, "Only accept cookies originating from the same server as the page being viewed." To turn off cookies completely select "Do not accept or send cookies."
6. Click the "OK" button at the bottom of the dialog window.

4.5.3   Removing cookies in Netscape

Netscape 4.x There are two options for deleting cookies with Netscape 4.x versions:

1. Use "Search" from the "Start" menu to locate the file called "cookies.txt", then edit this file (use Wordpad or Notepad for Windows systems).

2. Delete all lines except the first line that says "Do not edit."

OR

Delete the "cookies.txt" file and let the Netscape browser re-create it when needed.

Netscape 6
Simply use the menu sequence Tasks > Privacy and Security > Cookie Manager, then select "Remove cookies."

4.5.4   Disabling cookies in Internet Explorer

1. Open Internet Explorer.
2. From the Internet Explore menu bar select "Tools" and then "Internet Options."
3. The "Internet Options" window will open. From this window select the "Security" tab.
4. Select "Internet", by clicking on the picture of a globe.
5. Once Internet has been selected, click on the "Custom Level" button.
6. This will open the "Security Settings" Window.
7. From this Window, scroll down until you see the "Cookies" section.
8. Directly below this there will be a subsection entitled "Allow cookies that are stored on your computer."
9. Select "Disable" from the subsection.
10. Directly below this there will be another subsection "Allow per-session cookies (not stored)."
11. Select "Disable" from the subsection.
12. Click "OK" at the bottom of " Security Settings" window.
13. Click the "OK" button at the bottom of the "Internet Options" window.

4.5.5   Removing cookies in Internet Explorer

The process for removing cookies in Internet Explorer requires knowledge of several directories and operating system files. If done improperly the browser may become unstable. Knowledgeable users should consult their system administrator for instructions on how to remove cookies from IE.

4.5.6 Applications for Control of Cookies

There are a number of free and low cost applications available that assist users in controlling and removing cookies on their computer as shown is Table 3. These programs give users more options than those available through Web browser settings.

Table 3 — Cookie Management and Removal Tools[14]

Application	Cost	Web Site	Features	Browsers Supported
Cookie Cruncher 2.11	Free	www.rbaworld.com	Differentiates between AOL, IE, and Netscape cookies.	AOL 3, 4; IE3, IE4, IE5; Navigator 3.x, 4.x
Cookie Crusher 2.1	yes	www.thelimitsoft.com/	Intercepts cookies before they are stored on your hard disk, and it provides session statistics on most types of cookies.	IE3, IE4, IE5; Navigator 3.x, 4.x
Cookie Cutter PC 2.61	yes	www.ayecor.com/	Deletes all cookies or selects individual cookies for deletion or retention. It can also search a hard disk for cookies.	IE3, IE4, IE5; Navigator 3.x, 4.x
PC Cookie Pal 1.5	yes	www.kburra.com/	It handles IE4 shell integration, monitors current sessions, and lets cookies to be accepted or rejected on a session basis.	IE3, IE4, IE5; Navigator 3.x, 4.x

---

[14] Certain commercial products are described in this document as examples only. Inclusion or exclusion of any product does not imply endorsement or non-endorsement by NIST or any agency of the U.S. Government. Inclusion of a product name does not imply that the product is the best or only product suitable for the specified purpose.

Application	Cost	Web Site	Features	Browsers Supported
Cookie Server 1.01	yes	www.newfangled.san-jose.ca.us/	Manages persistent cookies and cookies in communication flow. It works through firewalls and supports multiple browser profiles in Navigator.	IE3, IE4, IE5; Navigator 3.x, 4.08; Opera 3.0
Cookie Terminator	yes	www.4developers.com/	Single-screen interface with limited dialogs. Cookies can be detected automatically or manually, individually or en masse.	IE3, IE4, IE5; Navigator 3.x, 4.x

4.6   Internet Proxies

Another method of increasing security and privacy is by using a third-party proxy service that allows users to surf the Web and e-mail anonymously. Depending on the service, proxies provide additional security features such:

- Encryption of web pages

- Protection from cookies

- Removal of scripts and other executable code (ActiveX, Java, etc.) imbedded in Web pages and e-mail.

Many of these services are available for free or for a nominal charge.

When using a proxy to surf the Web all requests for Web pages are made to the proxy server. The server then requests the Web page on behalf of the end user. Once the proxy receives the page, it forwards it to the end user (sometimes encrypted). This process provides several benefits. The Web server that provides the requested content only "sees" the proxy; it does not "see" the end user and thus cannot record or track the end user. Information transmitted from the proxy to the user may be encrypted and, therefore, cannot be intercepted. (The traffic is between proxy and the target Web server is not generally encrypted unless the target Web server offers encryption.) The proxy server can also analyze the content of the page prior to forwarding it, and can be configured to delete any cookie programs or active code that may be embedded in the page. Note that encrypting proxies may be incompatible with the organization's firewall and virus protection. If e-mail is encrypted in transit to and from the central office mail server, the server's virus protection software will not be able to detect the presence of viruses or other malicious files or attachments. Figure 7 depicts the proxy process.
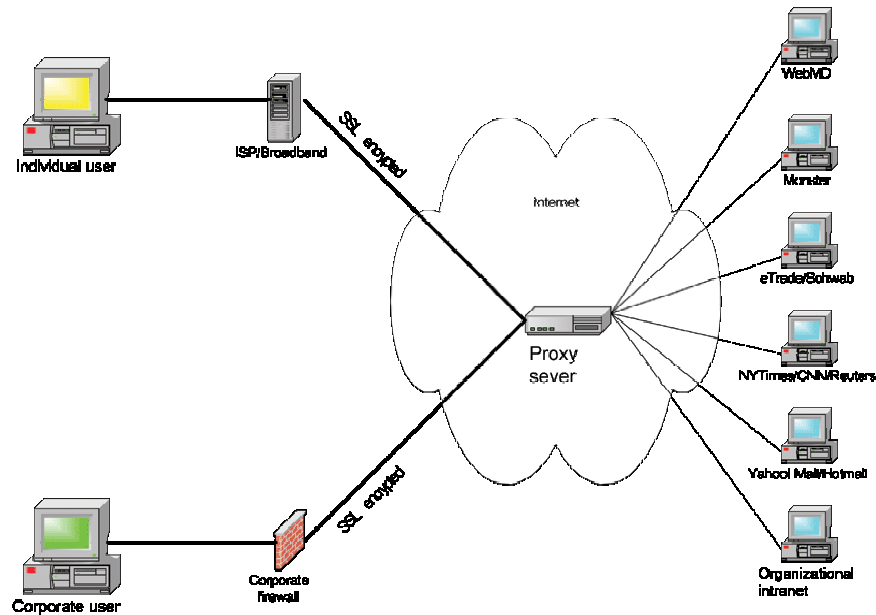
Figure 7 — Web Proxy Example

Before choosing a proxy service it is important to understand the services it provides:

- What is the cost?

- Does the service provide encryption between your computer and the proxy server?

- Does it offer the option of removing Active X, Java, and JavaScript?

- How are cookies handled (e.g., block all, block only profiling, or delete after each session)?

- Is it compatible with the Web sites you frequent?

Although proxy services are useful, they have limitations. Proxies can have performance issues as the additional overhead of using a proxy can slow access. The degradation in performance is generally due to encryption and the extra "step" of going through the proxy. Some web sites block proxy servers from accessing their content. Even when access is granted, proxies are often incompatible with certain Web sites. Sites with significant interactive content and dynamically generated pages are less likely to be compatible with a proxy.

Table 4 lists commonly used third-party proxy services. Services and costs associated with these proxies change regularly.

Table 4 — Web Proxy Services[15]

---

[15] Certain commercial products are described in this document as examples only. Inclusion or exclusion of any product does not imply endorsement or non-endorsement by NIST or any agency of the U.S. Government. Inclusion of a product name does not imply that the product is the best or only product suitable for the specified purpose.

Service	Web Site	Web Proxy	Anonymous E-mail	Encryption	Filters Cookies	Filters Active Code	Cost
Anonymizer	http://www.anonymizer.com/	✓		Partial	✓	✓	free
Anonymizer	http://www.anonymizer.com/	✓	✓	✓	✓	✓	yes
HiddenSurf.com	http://www.hiddensurf.com/	✓		✓	✓	✓	yes
Orangatango	http://www.orangatango.com/	✓		✓	✓		yes
Ponoi[16]	http://www.ponoi.com/	✓		✓	✓		free
PrivacyX	https://www.privacyx.com/		✓	✓			free
SafeWeb	https://www.safeweb.com/	✓		✓	✓	✓	yes

4.7   Summary Recommendations

Web browsers should be configured to limit vulnerability to intrusion. Web browsers also represent a threat of compromise and need some additional configuration beyond the default install. Browser plugins should be limited to only those required by the end user. Active code should be disabled or used only in conjunction with trusted sites. The browser should always be updated to the latest or most secure version. Privacy is always a concern with Web browsers and the two greatest threats to this privacy are the use of cookies and monitoring of Web browsing habits of users by third parties. There are a variety of ways of addressing cookies that range from disabling to selective removal using a variety of third-party applications. Internet proxies that encrypt all data protect home Web surfers from monitoring and allow them to use both the Web and e-mail anonymously.

---

[16] Ponoi presently supports only Windows machines that are running Internet Explorer 5.0 or later.

5   Securing PC Configurations

Information security risks can be broadly categorized into the following three types: *confidentiality, integrity,* and *availability*, which have the appropriate mnemonic "CIA."

Confidentiality refers to the need to keep information secure and private.   For most users, this category includes confidential memoranda, financial information, and security information such as passwords.   A personal computer (PC) used as a home office computer may also contain company proprietary information or trade secrets.

Integrity of information means that information remains unaltered by unauthorized users. For example, most users want to ensure that bank account numbers cannot be changed by anyone else, or that passwords are changed only by the user or an authorized security administrator.

Availability refers to the need that information be available for use when needed. The previously described denial of service attacks were assaults on the availability of Web servers owned by large commercial enterprises.   For broadband users, concern for availability includes both ensuring that their own systems are not disabled by intruders, as well as preventing intruders from hijacking systems for use in attacks against other systems.

Vulnerabilities can arise in a number of ways including: system configuration problems, software defects, and errors. Default configurations for most PCs are insecure. While this presents less of a problem for dial-up connections where users have reduced exposure to risk, default configuration should be avoided. Certain simple configuration options can make a big difference in reducing system vulnerability.

5.1   Strong passwords

So many computer tasks involve passwords that it is essential to develop a habit of choosing passwords that are not easily guessed or cracked.   Password cracking programs are widely available on the Internet.   Cracking programs use a dictionary of thousands of words and names, seeking to find one that the user has selected for a password. Dictionaries of 500,000 passwords are reported, and an intruder can try all of them in an overnight run. Common names of people or pets are the first passwords tried, because they are frequently used as passwords. Ordinary words are tried next, followed by words and names with one or two digits tacked on at the end. Use at least eight characters, including two or more digits. and characters. Digits and characters should be placed in random positions between letters, not just at the beginning or end.   Also password crackers will attempt common substitutions of numbers and characters for letters (e.g., h4ckm3 for hackme, r@ts for rats, p001 for pool, etc.).   A complicated password may be harder to remember, so most users will keep a written record of their passwords. This practice is much safer for the home user than it might be in an office, since presumably strangers will not have access to your home office.

5.2   Securing File and Printer Sharing

Both Windows and Macintosh operating systems have file and printer sharing features that allow complete access to files and printers from other machines on a local area network. While appropriate for a secure private network, these features are extremely helpful to an attacker if accessible from the Internet. For example, an intruder could modify or delete files and eventually compromise a system. The simplest (and most secure) solution to mitigate this vulnerability is to disable these features. In certain cases, a cable modem or DSL provider will disable these options when the connection is installed, but users should verify that this has been done and make corrections as required.

Disabling file and printer sharing for Windows 95/98/Melinimum Edition (ME)

1. From the "Start" menu, choose "Settings" > "Control Panel."
2. Click on the "Network" icon and a window will appear.
3. Click on the "Configuration."
4. Click on the "File and Print Sharing" button.
5. Ensure that "I want be able to give others access to my files" check box is unchecked.
6. Ensure that "I want to be able to allow others to print from my printers" check box is unchecked.
7. Click OK, then OK again on the next panel for any changes to take effect. The computer does not need to be restarted.

Disabling file and printer sharing for Windows 2000/XP

1. From the Windows Desktop using the right mouse button, click on "My Network Places".
2. From the "Network and Dial-up Connections" window that appears, double click on "Local Area Connection."
3. Click on "Properties."
4. From the "Local Area Connection Properties" window that appears, scroll down to "File and Printer Sharing for Microsoft Networks" and ensure that the check box next to this item is "unchecked" (if the item does not appear then file and printer sharing had not been enabled which is also secure).
5. Click "OK" and close the next panel for the changes to take effect.

Disabling file and printer sharing for Macintosh.

1. Open "Sharing Setup" control panel.
2. In the "File Sharing" section of the window, ensure that file sharing is off.
3. A dialog box will appear with text stating: "How many minutes until file sharing is disabled?" Enter "0" and click "OK."

5.3   Reducing Operating System and Application Vulnerabilities

Failure to keep operating system and application software up to date is the most common mistake made by both home users and professional information system professionals. Unfortunately despite extensive testing, operating systems and applications are released

with "bugs" (errors in the software) that affect security, performance and stability. These are generally discovered only after a large number of users begin using the software and hackers attempt to compromise it. Once a bug is discovered, the software manufacturer often releases a piece of software to fix the bug. This software is often called a patch, hotfix, or service pack.

Unfortunately, despite the importance of keeping software up-to-date, many users and professional system administrators do not install the latest patches. The Code Red worm exploited a vulnerability that was well-known and for which a patch already existed. It was the failure of Web server administrators to upgrade their servers that greatly contributed to the virulence of Code Red.

Until recently, applying patches was not user-friendly. Manufacturers have made this process easier by allowing user to download fixes from their Web sites. With the explicit instruction and at times partially automating the process for ease of use.

5.3.1   Operating System Updates

Linux. Linux updates can be found at a variety of Internet sites, but care must be taken in choosing a reliable site. Generally, it is recommended that downloads are taken from the distributor of your particular version of Linux[17].

- Red Hat: http://www.redhat.com/apps/download/

- Mandrake: http://www.linux-mandrake.com/en/security/

- SuSE: http://www.suse.de/en/support/download

- VA: http://www.valinux.com/support/

Macintosh. Apple offers an automated process for updating the Mac operating system through a Software Update feature. Patches and updates are also provided at http://www.info.apple.com/support/downloads.html.

Windows 95. To find updates for the Windows 95 operating system, visit http://www.microsoft.com/windows95/downloads/Default.asp.

Windows 98, ME, 2000 and XP. To update Windows 98/ME/2000/XP, click on the "Start" button and select "Windows Update." This is shown in Figure 8. This will launch Microsoft Internet Explorer, which will connect to the Windows Update Web site (http://windowsupdate.microsoft.com/). This site will ascertain what patches are required for your system. You can then download the patches you require. After the download, the patches will automatically install on your system. For systems that require several patches it may be necessary to repeat this process several times as the patches may need to be installed sequentially (the update site will alert you if this required). The Windows Update

---

[17] Certain commercial products are described in this document as examples only. Inclusion or exclusion of any product does not imply endorsement or non-endorsement by NIST or any agency of the U.S. Government. Inclusion of a product name does not imply that the product is the best or only product suitable for the specified purpose.

will also update most other applications included with the Windows operating system including Explorer, Media Player and NetMeeting.
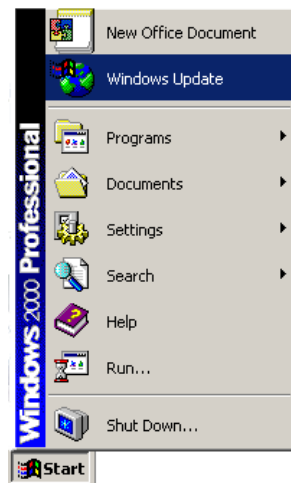

Figure 8 — Windows Update Feature

See Appendix C for more information on using the Windows Update feature.

5.3.2   Application Updates

Although there are limited network vulnerabilities associated with most applications (with the exception of Web browsers and e-mail programs), you should keep applications current.

Microsoft Office. Microsoft provides a Web based automated update process for most versions of Microsoft Office at http://office.microsoft.com/productupdates/.

Word Perfect Office. Updates for the Word Perfect Office suite and other Corel products can be found at http://www.corel.com/support/downloads/index.htm.

5.3.3   Browser Updates

As one of the most widely used applications, Web browsers can be a significant source of security vulnerabilities. Browser weaknesses are shared by hackers rapidly on the Internet when they are discovered, and the presence of Web browsers on almost every PC makes them a popular target. Adding to this vulnerability is the fact that a Web browser's primary purpose is to communicate with other machines, thus exposing them to greater risks. Software manufacturers release new browsers and patches regularly, and most security flaws are corrected in new releases, so most vulnerabilities can be avoided by periodically downloading the latest patch or browser version. The versions and patches are provided at the following sites:

- **Microsoft Explorer:** http://www.microsoft.com/downloads

- **Mozilla:** http://www.mozilla.com/

- **Netscape Navigator:** http://home.netscape.com/ – click on "Downloads"

- **Opera:** http://www.opera.com/support/ (free and paid versions)

5.4 Virus Checkers

Nearly all computer systems are susceptible to viruses, Trojans and worms[18] if they are connected to the Internet, use removable media (e.g., floppy disks and CD-ROMs), allow unsupervised access to users, or use shareware or pirated software (warez).

A computer virus is a string of code developed for malicious purposes that attaches itself to another computer program or document. Once it is attached, it replicates itself by using some of the resources of the co-opted program or document to replicate and attach itself to other host programs and documents. Three categories of viruses are prominent:

- **File Infectors** work by attaching themselves to program files, such as word processors and computer games. When the user runs an infected program, the virus adds itself to the computer memory so that it can infect other programs the user runs. File infectors were the most common type of virus but are nearly "extinct" due to changes in operating system design.

- **Boot-Sector Viruses** locate themselves in a specific part of the hard disk or floppy disk called the boot sector. Thus they are loaded into memory when the computer first boots up. Once in memory, the boot-sector viruses can infect any hard disk and floppy accessed by the user. With the advent of more modern operating systems and a great reduction in users sharing floppies there has been a major reduction in this type of virus. These are now relatively uncommon.

- **Macro Viruses** are the most successful due to the fact that they attach themselves to documents rather than disks or programs and users share the former far more often than the latter. Macro viruses can infect multiple platforms (e.g., Windows and Macintosh). They are currently the most dangerous of all viruses. They are common and spread rapidly.

Malicious code is not limited to viruses; there are several other types of malicious code that are generally detected by antivirus software even though the code is not strictly speaking a virus. Other categories of malicious code include:

- **Worms** are a type of malicious code particular to networked computers. They are self-replicating programs (unlike viruses which need a host program) that work their way through a computer network exploiting vulnerable hosts, replicating and causing whatever harm they were programmed to accomplish.

- **Trojan Horses, or Trojans** are designed to fool a user into thinking that they are benign. A Trojan horse is a program placed on a system by a hacker or installed unknowingly by the user that conducts malicious actions while hiding or pretending to do something useful.

- **Malicious Mobile Code** is a relatively recent development that has grown with the increased use of Web browsers. Mobile code is used by many Web sites to add functionality and is legitimate and includes ActiveX, JavaScript, and Java. Unfortunately, although it was initially designed to be secure, mobile code has

---

[18] These are all examples of malicious computer code (programs) that are sometimes collectively referred to as viruses even though they operate quite differently.

vulnerabilities that allow entities to create malicious programs. A user can infect a computer with malicious mobile code just by visiting a Web site.

The impact of a virus, Trojan horse, worm, or malicious mobile code can be as harmless as a pop-up message on the computer screen or as destructive as deleting all the files on a hard drive. With any malicious code, there is also the risk of exposing or destroying sensitive or confidential information.

Many antivirus applications are available to detect viruses, Trojans and worms contained in e-mails, floppies, CD-ROMs, hard disks, and documents. Certain antivirus applications also detect malicious mobile code from Web sites. No matter what type of virus detection program is being used it cannot offer its full protection unless it has an up-to-date virus identification database (sometimes called virus signatures) that allows it to recognize known viruses. If the virus detection program is not up-to-date, it will not be able to recognize a new virus. To detect viruses, antivirus software compares file contents with the known computer virus signatures, identifies infected files, and repairs them if possible, or quarantines (block access) them if not. More sophisticated programs also look for virus-like activity in an attempt to identify new or "mutated" viruses that would not be recognized by the current virus detection database. While not perfect, this feature can provide an additional layer of protection with the cost of occasional false positives.

5.4.1   Recommended Antivirus Software Configuration

All computers should have an antivirus program installed. Today, viruses represent a greater threat than previously. However, if the antivirus program is not properly configured, it cannot offer full protection. Ensure that the antivirus software is configured to:

- Initialize with the boot of the operating system (enabling it to scan the "boot sector" and other critical system files)

- Run in the background and automatically scan all incoming files (this would include downloaded files (mail, HTTP, FTP, etc), files loaded from removable media (floppy, CD-ROM, Zip, etc.) and files copied or loaded from the local area network (LAN) (share drives, file server, etc.). This option is often called "Auto-Protect", "Auto-Detect", and other similar names

- Enable Web or browser protection. While not all antivirus programs offer this feature, it should be enabled, if available, as it offers protection against malicious mobile code that is sometimes included with content from certain Web sites.

- Configured to automatically update virus signatures on a weekly basis. If this option is unavailable, then the signatures should be updated manually on a weekly basis. When there is an outbreak of a particularly virulent virus it is wise to update immediately to protect your system from the virus.

- Configured to attempt to recognized unknown or "mutated" viruses not contained in the virus signature database file. This feature is often called SmartScan, Heuristic Scan, etc.

5.5　Protecting Yourself from E-mail Worms and Viruses

Computer worms and viruses spread by e-mail and other means and are becoming a common hazard for users. As discussed previously, the term "virus" usually applies to executable code that attaches itself to other programs. A "worm" is spread primarily through e-mail, but may also travel through file sharing software (such as Gnutella and Napster), instant messaging, and Web file downloads. Malicious e-mail attachments such as the "love bug" (or "I love you") and "Melissa" viruses routinely make headlines. Some of these programs are merely nuisances, spreading copies of themselves to as many users as possible. Others are truly malicious, deleting files or reformatting PC disk drives. The "Magistr" virus/worm was designed to overwrite the Complementary Metal Oxide Semiconductor (CMOS) and Flash Basic Input Output System (BIOS) of PCs; once these are damaged, it becomes impossible to even reboot the machine. Both types are damaging; even the nuisance viruses cost money for companies and government agencies that must dedicate resources to removing them.

Most organizations have installed defenses against viruses in their internal systems. E-mail with suspicious executable attachments is rejected at the corporate firewall, virus scanners are used on e-mail that is accepted, and desktop systems have additional antivirus software installed. Telecommuting employees will have these same protections if their e-mail is sent and received by the corporate server, but desktop protection is the user's responsibility. Some additional precautions can reduce the chance of damage resulting from malicious e-mail:

- Use desktop system security software. Install and configure a virus scanner to inspect e-mail. If possible, obtain a virus scanner that automatically scans e-mail attachments. Update the virus scanner at the beginning of each workweek, or use virus-scanning software that automatically updates itself when you are connected to the Internet.

- Delete e-mail messages with attachments without opening them if received from an unfamiliar source. Develop the habit of reviewing e-mail subject lines and removing questionable messages before starting to read the body of the e-mail. Virus creators rely on users to open the first in a list of e-mails, then blindly clicking "next" to step through them one by one. By the time the user has opened the malicious e-mail, it is too late to prevent damage.

- Even if you recognize the sender of a message, do not open it if it seems suspicious. A number of users avoided the "love bug" because the subject line–"I love you" was obviously questionable when received from a business associate. Remember that e-mail viruses propagate by replicating and sending copies to everyone in an infected host's e-mail address book.

5.6　Spyware Removal Tools

Spyware is an application is installed on a user's PC by manufacturers and/or market research companies that communicates with its home site usually unbeknownst to the user. Spyware programs have been discovered to be installed with some shareware or freeware programs, children's games and by certain Web sites. Users are often not notified of this hidden functionality, or else it is often buried in the license agreement. News reports have accused various spyware programs of inventorying software on the user's system, collecting or searching for private information, and then periodically sending the information back to the home site. Uninstalling the software that delivered the spyware

often does NOT remove the spyware itself, although removing spyware often disables the application that installed it.

Spyware can gather just about any type of information on users that the computer has stored. The most common type of spyware is installed by shareware/freeware programs that are supported by advertisers. In this instance, the spyware application monitors where the user goes on the Internet and sends this information back to the company that created it (generally for marketing purposes).

Spyware is not readily detectable by the average user and can be difficult to remove. However, programs have be been developed to assist the user in this process. Please note that the removal of spyware may have an adverse effect on the program that installed it. This tends to be truer for shareware/freeware applications than for commercial applications. There are two types of spyware removal programs: those created by a spyware company to remove their particular application, and those that are created by third parties. Two freely available spyware removal tools are listed in Table 1.

Table 5 — Spyware Removal Tools[19]

Application	Web Site	Detects and Removes
Ad-Aware	http://www.lavasoftusa.com/	Adware, Alexa 1.0-5.0, Aureate 1.0-3.0, Comet Cursor 1.0-2.0, Cydoor, Doubleclick, DSSAgent, EverAd, EzUla, Expedioware, Flyswat, Gator, Hotbar 1.0-2.0 OnFlow, NewDotNet, TimeSink 1.0-2.0 and 5.0, Web3000, Webhancer
SpyBlocker	http://www.morelerbe.com/	Does not remove the spyware software but blocks its access to the Internet. This is useful if you need the functionality of a spyware-enabled product but do not want to be spied on.

A number of companies have created programs specifically for removing the spyware they developed. Table 6 lists some of these (free).

Table 6 — Specific Spyware Removal Tools

Application	Web Site	Removes
Mattel (The Learning Company)	http://support.learningco.com/brodcastpatch.asp	Interactive broadcast utility
Aureate/Radiate	http://www.radiate.com/privacy/remover.html	Aureate and Radiate

There are also several databases of known shareware/freeware programs that include spyware. You can download one of these programs to check whether or not the program you are considering installing contains a known spyware program (see Table 3).

---

[19] Certain commercial products are described in this document as examples only. Inclusion or exclusion of any product does not imply endorsement or non-endorsement by NIST or any agency of the U.S. Government. Inclusion of a product name does not imply that the product is the best or only product suitable for the specified purpose.

Application	Web Site	Cost
Spychecker	http://www.spychecker.com/	Free
Spy Chaser	http://camtech2000.net/	Free

5.7   Encryption Software to Protect Privacy

Encryption is one of the most powerful methods of protecting data. It is the process of making decipherable information indecipherable through a sophisticated mathematical conversion process.   Decryption takes encrypted information and makes it comprehensible again. There are three components to the encryption/decryption process.

1.   The information to be encrypted/decrypted

2.   The mathematical encryption/decryption process (the encryption algorithm). The encryption/decryption process is publicly known; the security of data encrypted with a public algorithm depends on the strength of the mathematical process and the encryption key. The advantage of publicly available algorithms such as NIST's Data Encryption Standard (DES) and new Advanced Encryption Standard (AES) is that they have been scrutinized extensively by some of the world's best cryptographers, so you have greater assurance of the encryption scheme's strength.

3.   The encryption/decryption key(s). The encryption/decryption key(s) is (are) a data string that is (are) mathematically combined with the information (clear or encrypted) by the algorithm to produce the opposite version of the data (encrypted or clear).

There are two primary types of encryption: *secret key* (symmetric) encryption and *public key* (asymmetric) encryption.   Secret key encryption is the traditional method of encryption. In this type of encryption, the same key is used to encrypt and decrypt the message. The single key has to be kept secret in order for the encryption to be secure as any party with the key can decrypt the data. This is the method that has been used for centuries by militaries and governments. Figure 9 shows a secret key encryption and decryption process.

Encryption
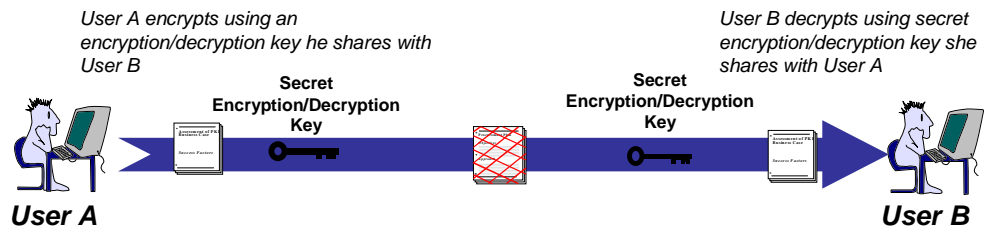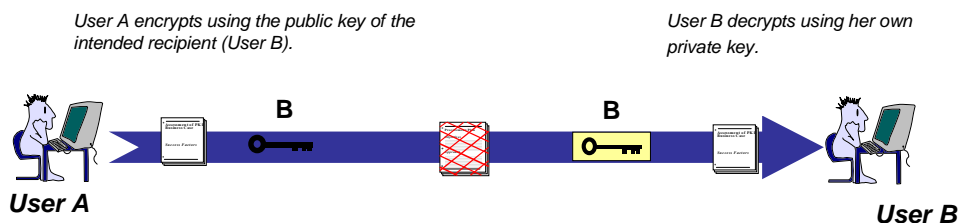

User A encrypts using an encryption/decryption key he shares with User B

Secret Encryption/Decryption Key

Secret Encryption/Decryption Key

User B decrypts using secret encryption/decryption key she shares with User A

User A

User B

The greatest limitation with secret key encryption is the requirement to keep the key secret. For example, how do two parties who wish to communicate securely exchange a secret key without compromising it? On traditional military and governmental systems, there are secure and dedicated channels for which to transmit the key securely. On the Internet, however, there is no secure channel to transmit a secret key securely. Another limitation with secret key encryption is that you need a secret key for each party to who you wish to communicate. If a secret key is shared with more than one party, those parties could eavesdrop on communications not intended for them but employing the same key. This limitation becomes critical if you wish to communicate securely with more than a few parties. For example if you wished to communicate with 100 users securely you would need 100 keys and each of those people in turn would need 100 keys.

Public key encryption addresses these limitations. With public key encryption there are two keys. One key is used to encrypt the data and the other is used to decrypt the data. The key that is used to encrypt cannot decrypt the data and vice a versa. Now a secure channel is no longer required to transmit the encryption key. Since the key that encrypts cannot decrypt, it can be sent over an unsecured channel. Even if a malicious third-party intercepts the encryption key, it cannot use it to decrypt messages. Only the second key, which is kept private, is able to decrypt the message. Also, since you can freely share your public key with more than one party (since it cannot be used to decrypt) each party needs only two keys (one public and one private) to communicate with multiple parties securely. E-commerce and most secure communications over the Internet could not take place without public key encryption. Most Internet secure encryption schemes rely on hybrid encryption schemes that employ both secret and public key encryption. Figure 10 provides an example of public key encryption.

Encryption

User A encrypts using the public key of the intended recipient (User B).

User B decrypts using her own private key.

User A

B

B

User B

Notes: 1. The public key and private key are mathematically related numerical values.
                2. Security depends upon the secrecy of the private keys and the authenticity of the public keys.

Figure 10 — Public Key (Asymmetric) Encryption

Encryption is important for both data transmission and data storage. Encryption is critical for transmission whenever sensitive data is being transmitted over a network that is insecure (i.e., the Internet). Encryption is important for storage whenever the data is subject to compromise. It is good to encrypt stored data when a machine is shared with between multiple users and for laptops that are often a target for thieves (encryption will not get your laptop back, but it will protect the data from compromise).

There are many commercial and freeware products available that will allow you to encrypt e-mail and hard disks. Many new operating systems include a standard hard disk encryption feature as standard. Encryption products are increasingly easy to use and should be considered for situations where sensitive and critical data are subject to compromise.

Before using encryption there are limitations to consider. You need to appropriately secure your encryption key or else the key and encrypted data are subject to compromise. To secure encryption, it is generally most secure to store the key on removable media that can be protected with a strong password. If the key is stored on the hard drive with the encrypted data, a strong password becomes critical. Also, encrypted data can complicate data backup and restoration. For example, if the key is not backed up the backed-up data is useless.

There is a wide variety of different encryption products available. NIST maintains a list of cryptographic modules that have been validated against Federal Information Processing Standard 140-2. This standard is applicable to all Federal agencies that use cryptographic-based security systems to protect sensitive unclassified information in computer and telecommunication systems (including voice systems) as defined in Section 5131 of the Information Technology Management Reform Act of 1996, Public Law 104-106. See http://csrc.nist.gov/cryptval.

Some products and protocols provide encryption only during storage of data (e.g., saving to a hard disk, floppy, or CD-Recordable. An example of this type is Microsoft's Encrypting File System (EFS), which is included with Microsoft Windows 2000 and XP. These products encrypt the data, as it is stored onto media. This means that even if an attacker compromises a host via a remote attack or is in physical possession of the media, he or she will be unable to read the encrypted data, provided the keys are not stored on the system. However these products and protocols do not provide a means to protect data as it is being transmitted from one location to another. It is also important to ensure that there is a safe and secure method to recover the data if the person holding the key loses it. The corporate office should have some means of key recovery or data recovery to prevent potential loss of valuable data.

Other products encrypt only during transmission (e.g., an e-mail or web communications). When data is encrypted during transmission, the data at each end of the transmission is unencrypted but get encrypted just prior to transmission. These are useful for transmitting data across unsecured communications links. Even if an attacker intercepts the data he or she will be unable to decrypt and read the message. They do not however protect the data once it has been received and so a hacker may attack the repository where the data is received and stored. Examples of these types of products and protocols are Secure Multipurpose Internet Mail Extensions (S/MIME) and Secure Socket Layer (SSL).

There are also products that combine both of these capabilities. A commonly used example is Pretty Good Privacy (PGP)[20]. Which provides the ability to encrypt e-mails and data stored on media such as hard disks. The software you choose should be based on your own personal requirements and what products or protocols that are support by you organization. For example many Virtual Private Network (VPN) client software provides some or all of the capabilities discussed above and may be provided by your organization.

---

[20]See The International PGP Home Page http://www.pgpi.org/

5.8   Summary Recommendations

Operating system configuration options should be selected to increase security. The default configuration of most home operating systems is generally inadequate from a security standpoint. File and printer sharing should almost always be disabled. The operating system and major applications should be updated to the latest and most secure version or patch level. All home computers should have an anti-virus program installed and configured to scan all incoming files and e-mails. The anti-virus program needs to have its virus database updated on a regular basis. Another concern for many home users is the surreptitious installation of spyware by certain software applications. This spyware while not intended to be malicious, reports information on a user (generally without their knowledge) back to a third-party. This information could be general information about their system or specifics on their Web browsing habits. There are now a variety of programs available for detecting and removing this spyware.

6   Home Networking Technologies

By the end of 2000, according to International Data Corp. (IDC), about half of all U.S. households had a computer, and more than 20 million of those had more than one. In fact, market research shows that current PC owners are buying most of the new computers. This means that multi-computer households are becoming fairly common. Linking multiple computers on a network introduces new security considerations. For example, previous chapters explained reasons to turn off file and print sharing capabilities for an individual PC on a broadband connection. If a home network is set up, users may want to be able to share files and printers across the network. This section discusses methods of setting up these and other network services securely.

Many of these multiple-PC households have, or soon will have, a home network that will allow the multiple computers to communicate. Home networking permits:

- Sharing a single printer between computers

- Sharing a single Internet connection

- Sharing files such as images, spreadsheets, and documents

- Playing games that allow multiple users to participate in the game from different computers

- Transmitting the output of a device like a DVD player or Webcam to other computers.

There are several different technologies for networking home computers. Each has its own strengths and weaknesses that will be discussed in greater detail below. The most popular techniques for home networking include:

- Wire your house with data cables (e.g., Ethernet)

- Install wireless networking (e.g., 802.11b)

- Link computers through existing home power lines

- Link through existing home phone wiring

Each of these methods has advantages and disadvantages. All of these methods require configuring computers to share printers, files, Internet connection, and to set up a particular level of security. Particular types may require the installation of wiring and/or additional hardware inside the computer.

6.1   Ethernet Networking

Ethernet is the most popular networking system available today. The equipment needed for an Ethernet-based network can be as simple as two network interface cards (NICs) and a cable, or as complex as multiple routers, bridges and hubs. It is this versatility that makes it useful to businesses and home users.

Ethernet is available in three speeds: 10 Mbps, 100 Mbps (FastEthernet), an 1 Gbps. Most network interface cards (NICs) are capable of operating at either speed, but check to be sure before purchasing. Generally, it is best to purchase cards capable of the 100-

Mbps data rate, as the difference in cost is minimal. A 10-Mbps card costs about $15 to $40, and a 10/100-Mbps card costs about $25 to $50.

There are two different methods to connect Ethernet cards: coaxial cable (similar to TV cable) and Category 5 cabling. Coax was once the more popular of the two, but today almost all installations use Category 5 because it is easier to configure. Category 5 uses a cable that resembles a telephone cable. A cable runs from each computer and connects to a hub. A basic hub for a home network is a small box that typically costs from $30 to $100 (depending on its speed and how many connections it can support). The hub takes the signal from each computer and sends it to all of the other computers connected to it. Hubs come in several sizes, indicated by the number of ports available—a four-port hub can connect four computers, an 8-port hub can connect up to eight computers and so on. A cable/DSL router/hardware firewall (see section on personal firewalls) usually has a four-port Ethernet hub built in.

To connect the computers, an Unshielded Twisted Pair (UTP) Category 5 cable is needed. This type of cabling is designed to handle the 100-Mbps speed needed by FastEthernet. The RJ-45 connector at the end of the cable looks very similar to the RJ-11 connector on a phone cord but is slightly bigger (and not compatible). You can buy Category 5 cables in standard lengths with the connectors attached. If you install Category 5 cabling in the walls of your house, the cable can be purchased in rolls, cut to length, and connected to special RJ-45 wall boxes. Unless you have done this type of installation before, you will probably want to hire a professional.

If you are comfortable running the cables along the floor, you can install an Ethernet network for two computers in your home for $100 or less, which includes the cost of two Ethernet cards, a small hub and two cables. Each additional computer will cost about $30 to $40 to connect using inexpensive network cards. [Note: If you want to connect just two computers, you can avoid the hub and buy what is called a crossover Category 5 cable. With a crossover cable, you directly connect one NIC card to the other without a hub. This only works for two computers—to connect more than two you need a hub.]

Ethernet has many advantages:

- Fastest home-networking technology (up to 100 Mbps)
- Relatively inexpensive (if the computers are in the same room or appropriate wiring is already installed in your home)
- Extremely reliable
- Easy to maintain
- Supports a large number of devices on a network
- Supports nearly all types of computers and operating systems
- Widely available technical support and information.

Ethernet also has a number of disadvantages:

- Additional equipment (e.g., hub, switch, router, etc) required when connecting more than two computers
- Expensive if wiring and jacks need to be installed
- Set-up and configuration can be difficult
- Installation on desktop machines often requires assembly

- Technical jargon and the number of options can be confusing for beginners.

6.2   Phone-Line Networking

Phone-line networking is easy to install, inexpensive and fast, and does not require any additional wiring since it uses your house's existing telephone wiring for computer networking. Phone-line networking, most commonly referred to as HomePNA, is based on the specifications developed by the Home Phone Networking Alliance (HPNA). The HPNA is a consortium of key networking technology companies that created a phone-line standard for the networking industry. HPNA 1.0, the original version of the standard, operated at 1 Mbps. The current specification, HPNA 2.0, is based on improved technology and operates at a faster 10 Mbps (comparable to regular Ethernet).

HomePNA uses a method known as frequency-division multiplexing (FDM). FDM puts computer data on separate frequencies from the voice signals being carried by the phone line. FDM separates the extra signal space on a typical phone-line into distinct data channels by splitting it into uniform chunks of bandwidth. To better understand FDM, think of radio stations—each station sends its signal at a different frequency within the available band. In HomePNA, voice and data travel on the same wires without interfering with each other.   In fact, a standard phone-line has enough room to support voice, a high-speed DSL modem, and a home phone-line network.

HomePNA adapters come in two versions: internal card (PCI) or external universal serial bus (USB). You can buy kits consisting of HomePNA cards for two computers, an installation CD and all the necessary cables for about $90 to $110. The actual cost of implementing HomePNA depends primarily on the type of interface you buy for each computer: PCI cards cost about $45 to $55, while USB adapters range from $75 to $85. If you plan to use a laptop computer that does not have a USB port, you can either buy an USB-to-PCMCIA adapter ($50) or get a parallel-port USB adapter. USB interfaces have the advantage that they do not require opening your computer(s) to install a card.

There are a few things you should keep in mind when you set up a HomePNA network. First, most analog communication devices, such as telephones and fax machines, create signal noise. A little signal noise probably will not affect HomePNA traffic, but a lot of it could slow down or even stop network traffic. If you install a HomePNA network and your computers have trouble communicating, try inserting a low-pass filter between any phones or fax machines and their respective jacks. The low-pass filter will block noise without impeding the performance of your fax or phone. You can find these filters at most electronics stores.

Also, electrical fields generated by powered communication devices, such as cordless phones or fax machines, can introduce another type of signal noise. A different type of low-pass filter, inserted between the electrical wall outlet and the power cord for the device, can fix this problem.

The last potential issue is rare but much harder to fix. If you have a very large home, or one that has been renovated several times, you may have too much wiring between computers. All of this wiring will weaken the signal, causing it to fade out and lose strength. The result is that not enough of the signal remains if, and when, it reaches the other computer for that machine to process it. If this is the case, then you will either have to move the computers closer together or redo the wiring, at which point you may want to consider other home networking options.

HomePNA has several advantages:

- Easy installation

- Inexpensive

- Reliable

- Provides a consistent 10 Mbps even when phone and/or fax is in use

- Requires no additional networking equipment (such as hubs or routers)

- Supports up to 25 devices

- Provides enough bandwidth for most applications

- Compatible with other networking technologies

- Supports Linux, Macs and all versions of Windows.

HomePNA also has several disadvantages:

- Requires a phone jack close to each computer

- While 10 Mbps is adequate for most applications, it is still 10 times slower than Fast Ethernet (100 Mbps)

- Physical limit of 1,000 feet of wiring between devices, and the overall area of coverage should not exceed 10,000 square feet

- Will not work with the wiring in about 1 percent of U.S. homes

- In rare instances can cause interference with regular voice telephone service.

6.3   Power-Line Networking

Power-line networking uses the electrical wiring this is already installed in homes to create a network. Power-line networking, like telephone-networking, is based on the concept of "no new wires." The convenience is even more obvious in this case because while not every room has a phone jack, there will generally be an electrical outlet near a computer. Because it requires no new wiring, and the network adds no cost to your electric bill, power-line networking is often the most inexpensive method of connecting computers in different rooms.

The physical connection between each computer and the power-line network uses the computer's parallel port. A wall device is plugged directly into the electrical outlet (it will not operate properly if plugged into a surge protector).

A parallel cable is plugged into the wall device and into the parallel port of the computer. The power-line network must be the last item connected to the parallel port. For this reason, if you have anything else connected to the parallel port, such as a scanner or Zip drive, it must have a pass-through for the parallel port. Unless you have a second parallel port on your computer, your printer must be connected to the network through a wall device of its own.

Once the physical connections are made, installation of the software is generally straightforward. The software automatically detects all nodes (computers and printers) on the network. Whether your Internet connection is by cable modem, DSL, or dial-up

modem, the included proxy server software allows you to share the Internet with your other computers. You can easily add computers by simply plugging a new adapter in and installing the software. Additional printers can be added using the printer plug-in adapter.

Power-line networking has several advantages:

- Inexpensive

- Employs existing electrical wiring (electric outlets are typically found in every room in a house)

- Ease of installation.

Power-line networking has several disadvantages:

- Slower than Fast Ethernet installations with a maximum speed of 10 Mbps

- Performance can be impacted by home power usage or older wiring

- Supports only Windows-based computers

- Uses large wall devices to access an electrical outlet

- Requires that all data be encrypted for a secure network (network data can be transmitted to other location through the power lines leading from your house).

The segment of the home network market has seen significant change. Most new products use technology created by Inari and the Home Plug Powerline Alliance. Visit the Inari Web site (www.inari.com) and Home Plug Web site (www.homeplug.com) for a list of vendors that are currently selling power-line networking products.

6.4   Wireless Networking

Wireless networking is the fastest growing segment of the home networking market. Although it tends to cost more, the convenience of installation (no wires) and the ability to stay connected around the house and nearby yard is very attractive to home users. There are two wireless networking standards: HomeRF and IEEE 802.11b. Both offer different capabilities and features.

6.4.1   HomeRF

HomeRF is the current low-cost home wireless network. While its 1.6 Mbps bandwidth is less than that of the 10-11 Mbps speed of HomePNA 2.0, 802.11b, or even Ethernet, HomeRF 1.0 is still fast enough to allow transport of multiple MP3 audio streams while others on the network surf the Internet. Because the cost difference between HomeRF and 802.11b (see below) is quickly eroding, the more expensive alternative is a more viable option for most users.

HomeRF was designed specifically as a low-cost technology for wireless home networking. You do not need to use an access point with HomeRF networks, which is a cost savings compared to 802.11b. However, HomeRF's 1.6 Mbps bandwidth is a drawback, particularly with 802.11b's rapid drop in price.

The HomeRF wireless network protocol is called the Shared Wireless Access Protocol (SWAP), but is more commonly referred to as HomeRF. One of the main advantages of HomeRF over 802.11b is its capability to support four separate voice lines simultaneously. If you are not going to use your home network for voice content, but for data, however, HomeRF has to be compared to 802.11b on the basis of speed (bandwidth), cost, ease of installation, and compatibility with other networks—and it currently falls short for demanding home network applications.

For small home networks, HomeRF provides adequate performance with enough bandwidth to conduct multiple high-bandwidth usage activities simultaneously. The actual data rate is closer to 1Mbps than 1.6Mbps, which is still adequate for applications that do not require large amounts of bandwidth. The specification theoretically supports up to 127 users, though manufacturers recommend no more than 10 users on a HomeRF network. If you have a broadband Internet connection you can share it on a HomeRF network via an Internet Gateway, but if you have multiple simultaneous users and do heavy downloading or file transfers it is likely you will likely face bandwidth restrictions.

HomeRF is barely fast enough for playing raw CD audio across a network if only one user is active and is inadequate for streaming video content. In 2000 the FCC approved a higher bandwidth, 10 Mbps for HomeRF's SWAP specification, but the first products for this new version are not expected before the fourth quarter of 2001.

HomeRF wireless networking has several advantages:

- Inexpensive

- Does not require any additional wiring

- Ease of installation.

HomeRF wireless networking has several disadvantages:

- Slower than most other options

- Security risks inherent in all wireless networks (see next section wireless networking security issues)

- Only supports Windows-based computers

- Subject to interference from other household devices

- Requires that all data be encrypted for a secure network (see section below on security concerns of Wireless networks).

6.4.2   802.11 and 802.11b

If you are willing to invest the money in 802.11b components, you can move your PCs freely throughout your home and yard without being disconnected from the network. You can also add personal digital assistants (PDAs) to an 802.11b network with adapters. The appeal of 802.11b technology is increasing as the price has decreased.

Until recently, 802.11b wireless components have been prohibitively expensive for home use. Now, however, prices are dropping rapidly. The current price for 802.11b network adapters is approximately $100, with $75 a foreseeable target, and access points priced under $200 are now common. Even though 802.11b wireless networking remains a

relatively expensive technology to install in a home network, the cost differential is not as great as it was previously, which allows comparison on other features and benefits.

Setting up an 802.11b network is relatively easy, although the amount of difficulty is largely a function of the software included with the network interface cards. Since people who use notebook PCs with wireless network cards at their place of work often take the same computers home at night, it may be useful to have 802.11b at home as well, for relatively easy transition from office to home networks. Again, the software involved can make this transition easy (or difficult). Generally, the only step necessary is changing the content of a single identification field in adapter set up software for the 802.11b device to be able to look for an access point and local network with which to work.

One issue that affects the use of 802.11b networks is the potential for interference by Bluetooth wireless devices. The technology employed by 802.11b uses direct sequence spread spectrum technology in the 2.4GHz radio frequency. Bluetooth is a 2.4GHz frequency hopping technology used by certain portable devices, that allows Bluetooth devices within range (30 feet) to find each other. This becomes a problem when Bluetooth devices happen to hop on the frequency currently being employed by an 802.11b device. The interference problem does not cause the 802.11b network to fail, but can degrade the performance. In some cases, users might not notice, but in other instances, the effect of Bluetooth in the area could be a significant problem. Several companies are working on solutions to this interference, but at this point about 802.11b/Bluetooth interference has not been resolved.

Microwave ovens and 2.4GHz portable phone systems are other sources of interference with 802.11b networks. Generally maintaining 10 feet of distance between the access point and offending device(s) can avoid these problems and users may not be able to talk on a 2.4GHZ phone near the computer when using 802.11b networking.

Because the data transfer rate for an 802.11b network is comparable to that of HomePNA 2.0 (current) 10Mbps rate and to Ethernet networks, deciding between the technologies does not need to be governed by speed. You can stream DVD movies across a network at 10Mbps but that will not leave much bandwidth for other users. If you want to stream HDTV or uncompressed video (which require approximately 20Mbps and 30Mbps, respectively) on your network, Fast Ethernet will be required.

Using 802.11b in conjunction with other network technologies is appealing, although the cost will increase for mixed networks. If you already have a 10/100 or other variety Ethernet network, you'll find it easy to add a wireless network for remote (in the house) PCs, for notebook PCs, and for PDAs that are compatible with PC Cards.

802.11b wireless networking has several advantages:

- Bandwidth capable of supporting most home networks
- Does not require additional wiring
- Accessibility
- Ease of installation.

802.11b wireless networking has several disadvantages:

- Slower than Fast Ethernet
- Requires strong encryption to be secure

- Security risks inherent in all wireless networks
- Subject to interference from other household devices.

6.5   Wireless Networking Security Issues[21]

Because wireless networking broadcasts information that can be intercepted more easily than wired communications, a number of security concerns should be carefully considered before deciding on deployment of this technology. Hackers and other malicious parties now regularly drive around office parks and neighborhoods with laptops equipped with wireless network cards attempting to connect to any discovered wireless networks (this is practice is called "war-driving"). There are now web sites that publish the locations of discovered wireless networks (e.g., www.netstumbler.com). The range for many wireless devices for home use is 300 feet and this is growing as manufacturers introduce new products. Hackers often had larger antennas to their wireless network cards to increase the reception range of their cards.

Unfortunately a number of security vulnerabilities are associated with the 802.11b networking protocol:

- Sever Set ID (SSID) usually sent "in the clear" (e.g., unencrypted). SSID is a configurable identification that allows clients to communicate to the appropriate base station. With proper configuration, only clients that are configured with the same SSID can communicate with base stations having the same SSID. Unfortunately the Wireless Equivalent Privacy (WEP) encryption standard employed by 802.11b does not encrypt the SSID so if an attacker can receive your wireless network signal it is only a matter of time before they intercept your SSID. Once they have the SSID they can generally connect to your network unless other steps are taken (see section on mitigation techniques below).

- WEP encryption scheme is flawed. WEP can be configured in 3 possible modes: no encryption, 40 bit encryption and 128 bit encryption. Obviously no encryption is the weakest allowing anyone who can receive you wireless LAN signal to intercept your data. WEP encryption has a number of vulnerabilities that allow attackers to eventually compromise data encrypted only with WEP. Today, there are readily available tools to automate the process of cracking WEP encryption. These tools take a lot of network traffic (millions of packets) to get the WEP key. On most home networks this would take longer than most people are willing to wait. If the network is very busy however, the WEP key can be cracked and obtained in as little as 15 minutes. The fix for the WEP encryption is not slated to be addressed until 2002.

- Many wireless base stations have Simple Network Management Protocol (SNMP) enabled. If the community string (essentially a password) for this service is not properly configured an intruder can potentially read and write sensitive data on the base station.

---

[21] This section will focus on the 802.11b, the most popular wireless networking protocol, but much of the discussion will apply to other wireless networking technologies as well.

- All wireless technologies are subject to denial of services attacks. An attacker with the proper equipment can easily flood the 2.4 GHz frequency with spurious transmission so that the wireless network ceases to function.

Compounding the security risks inherent in wireless networks is that most base stations are configured in the least secure mode out of the box. This makes installation easier, but puts the onus of security on the home user installing the wireless network. Most base stations are delivered in the least secure mode possible:

- Most wireless base stations have the SSID set to a default value. These are well known and if not changed allows anyone who knows the default SSID value to connect to your wireless network.

- Many wireless base stations come configured in a "non-secure access mode" which allows any computer to connect to a base station with or without the appropriate SSID.

- Most wireless base stations come with WEP turned off. That is no encryption is being used. This allows even casual attackers to monitor your wireless network traffic. Even though WEP is weak it should still be used as it impedes all but the most determined attackers.

- Most wireless base stations come configured with well-known default SNMP community strings.

These vulnerabilities allow a number of different attacks to be perpetrated:

- Connect unauthorized hosts, typically a laptop or PDA, to your base station without authorization (depends on configuration, see section below on mitigation techniques)

- Intercept and monitor wireless traffic on your network (often even if encrypted)

- Hijacking existing sessions (e.g. it is possible for an expert attacker to take over your secure encrypted web based session with your online banking institution)

- Denial of service attacks (overwhelm the radio frequencies employed by the wireless network with spurious traffic).

- Attack another wireless client directly, by bypassing base station. If a wireless client, like a laptop or desktop, is running TCP/IP services like a web server or file sharing, an attacker can exploit any misconfigurations or vulnerabilities with another client.

Although a wireless network can never be made as secure and robust as a wired network, there are several steps that a user can take to better secure their wireless network:

- Use additional encryption beyond WEP. For example encrypted VPN, Secure Socket Layer (SSL) and Secure Shell (SSH) traffic is all encrypted before transmission and therefore is far less susceptible to compromise even if WEP encryption is not enabled or has been compromised by an attacker.

- Enable 128 bit WEP encryption (see vendor documentation).

- Change SSID to a hard guess password (include letters, numbers and characters).

- Enable any additional authentication schemes supported by your base station. Two common examples are authentication based Media Access Control (MAC) address or WEP authentication keys. If your wireless base station supports either of these protocols; configure them according to your vendor's documentation.

- Disable broadcasts of SSID in the wireless base station beacon message (see vendor documentation). In most default configurations the base station regularly broadcasts the SSID making it much easier for an attacker to intercept the SSID. Even when disabled, the wireless clients will transmit the SSID (albeit much less frequently), so a patient attacker will eventually get the SSID.

- Disable SNMP on wireless base station and wireless client(s) (see vendor documentation). SNMP allows for remote administration across the network, but for home use, it is safer to manage controls using a direct connection to the base station. (See vendor documentation for where to connect to USB or other port.)

- Ensure that the administrative password used to configure the wireless network base station is changed and difficult to guess (i.e., not a dictionary word and includes letters, numbers and characters).

- All wireless client computers should be treated as if they were directly exposed to the Internet. That means additional steps must be taken to secure these hosts. Ensure all clients with a wireless network card have:

  o A personal firewall installed (even if your network also has a firewall installed at its Internet connection)

  o File and printer sharing disabled

  o SNMP disabled

  o NetBIOS protocol disabled over TCP/IP (see vendor documentation)

  o All TCP services that are unnecessary disabled.

While there are risks associated with using wireless networks many can be mitigated with careful planning and configuration. For many users the benefits of wireless networks will outweigh the risks. However given the weaknesses of WEP encryption, any sensitive or proprietary data transmitted should be encrypted prior to transmission by other means (e.g., VPN, Pretty Good Privacy, SSL, SSH). Generally, with the proper precautions, users can safely use home wireless networks.

6.6   Summary Recommendations

Selection of wireless and other home networking technologies should be in accordance with security goals. A variety of home networking technologies have become available for

home users who wish to connect their home PCs together to share resources. Some of these technologies are the same as their office counterparts (e.g., Ethernet) and others are intended to specifically meet the needs of home users (e.g., phone- and power-line networking). While most of these technologies are secure, several represent a threat to security of both the home network and, sometimes, the office network. In particular, wireless networking has several vulnerabilities that should be carefully considered before any installation.

7   Virtual Private Networks

If a business needs to conduct secure communications between several different locations, a private network can be constructed by leasing or installing private communication lines. A less expensive and more flexible alternative is installing a Virtual Private Network (VPN) that uses the Internet as the transport medium and employs security measures to ensure that the communications are indeed private. Although the VPN's traffic crosses the Internet, VPN protection prevents unauthorized users from reading and/or modifying the traffic.

7.1   VPN Security

VPNs can provide some or all of the following types of protection:

- **Connectionless integrity:** a guarantee that the message that is received is the exact one that was sent, and no tampering has occurred. Why "connectionless"? This is because communications at the Internet layer follow a post office model (as opposed to a phone company model). Messages are sent from the sender to the receiver, but no attempt is made to ensure that they are received in order, or that any (or all) were in fact received. Integrity is provided through the use of a message authentication code (MAC) and a symmetric secret key. Two MACs that are commonly used for this purpose are HMAC-SHA-1 and HMAC-MD5.

- **Data origin authentication:** a guarantee that the message actually was sent by the apparent originator of the message, and not by another user masquerading as the supposed message originator.

- **Confidentiality** or **privacy:** a guarantee that, even if the message is "read" by an eavesdropper, the contents are not understandable, except to the authorized recipient. Confidentiality is provided through the use of an encryption algorithm and a symmetric secret key. Triple DES is a widely used encryption algorithm; NIST's newly defined Advanced Encryption Algorithm (AES) is expected to replace triple DES once it has been designated a Federal Information Processing Standard (FIPS).

- **Traffic analysis protection:** an assurance that an eavesdropper cannot determine who is communicating with whom or determine the frequency and volume of communications between specific entities.

- **Access protection:** control over which network resources can be accessed by telecommuters and what types of network traffic can be initiated by or exchanged with telecommuters.

Which of these protections are actually supplied by a particular VPN implementation depends on the configuration, access policies, and setup of the VPN.

7.2   VPN modes of operation

There are two basic modes in which VPNs can function for telecommuting: host-to-host or host-to-gateway. Host-to-host enables the telecommuter to conduct protected communications with one or more other hosts. In this case, each host would have to be equipped with a VPN client that can interoperate with the VPN clients on the other hosts. The more common scenario (host to gateway) involves a firewall or gateway (which we will refer to as a security gateway) that is VPN-enabled; it functions as a gatekeeper for the business network that the telecommuter wants to access. In this case, the telecommuter's host needs a VPN client that is compatible with the security gateway's VPN implementation. The telecommuter can then conduct protected communications with the hosts that reside on the network protected by the security gateway. Figure 9 illustrates this configuration. Solid lines #1 and #2 constitute a protected VPN between the telecommuter and the security gateway. The telecommuter can then send unprotected traffic inside the network, represented by dotted line #5, or protected traffic to other destinations outside the network, represented by solid line #3. If the employer's security policy allows, the telecommuter can also send unprotected traffic, represented by broken line #4. Alternatively, the security gateway's policy might prohibit that type of traffic and require the telecommuter to route all traffic through the gateway, as it would if the telecommuter's host physically resided on the internal network.

A gateway-to-gateway VPN is also possible, but this would not be appropriate for a telecommuter as it is employed between two or more office networks (e.g., headquarters and regional offices). Today's cable modems and cable/DSL routers will generally allow the traversal of VPN data (often referred to as VPN or IPsec pass-through mode), but they do not provide VPN capabilities and protections themselves.
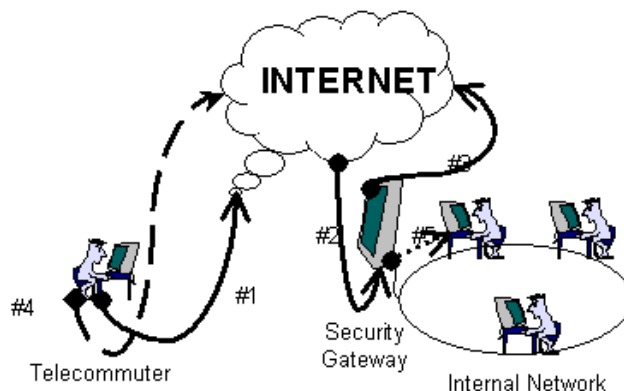

Figure 11 — VPN Example

7.3   VPN protocols

In an ideal world, a telecommuter could simply run a VPN client, confident in the knowledge that the protected traffic is secure. In today's world, however, the telecommuter

often needs to know numerous technical details about the VPN client and its underlying protocols. It is essential that the VPN client interoperate with other VPN clients or with the security gateway's VPN implementation. In addition, some VPN technologies are more secure and flexible than others. Within the same VPN technology, there can be a variety of features, usability, and interoperability.

A number of secure networking technologies are generally used to provide VPN protection. These include a number of standard protocols that have been defined by the Internet Engineering Task Force (IETF):

- **Internet Protocol Security (IPsec):** IPsec is the most widely used secure network protocol. It provides VPN capabilities at the Internet Protocol (IP) layer of communications. That means all types of Internet traffic can be IPsec-protected, independent of the specific applications that conduct the communications. The applications do not need to be aware of the protection and do not need to be altered in any way to enable it. IPsec's key management protocol, the Internet Key Exchange (IKE), is used to negotiate the secret keys that protect VPN communications, and the level and type of security protections that will characterize the VPN.

- **Secure Sockets Layer (SSL) or Transport Layer Security (TLS):** Originally developed by Netscape and known as SSL, the TLS protocol was subsequently adopted, renamed, and slightly modified by the IETF. It is a session-oriented protocol that provides security at the transport layer, a higher layer in the TCP/IP protocol stack than IP. It can more easily provide individual user-level access protection than the current IPsec. However, that comes at a price: Applications that use TLS must be modified for the purpose, and each individual session must establish its own TLS protection. Moreover, TLS can protect only applications that run over TCP. TLS is currently widely used to protect Web browser traffic.

- **Layer 2 Tunneling Protocol (L2TP):** L2TP is an extension of the Point-to-Point Protocol (PPP), which was developed to incorporate dial-up traffic into an IP network. PPP allows a dial-up user to connect with its destination and authenticate the user's identity through the use of an authentication protocol such as RADIUS. It then creates a PPP tunnel, encapsulating the phone link in an IP packet, enabling the non-IP phone traffic to act like any other Internet traffic. For users who dial into a local ISP that is not co-located with the network gateway, L2TP creates an extended tunnel that includes the PPP tunnel and the ISP-to-gateway leg, extending from the dial-up user to the network entry point. This enables the user to authenticate his/her identity directly to the network. However, L2TP does not include any mechanism for encryption or authentication of its traffic.

  A number of protection schemes have been suggested for the protection of L2TP traffic by IPsec, thus providing the facilities of a secure VPN. These schemes do, however, sacrifice some IPsec access control capabilities. L2TP is also used by some IPsec VPNs to fill in nonstandard areas within IPsec, such as the exchange of policy or configuration information between a telecommuter and a security gateway.

- **Point-to-Point Tunneling Protocol (PPTP):** PPTP is a predecessor to L2TP that shares L2TP's major goals. A version of PPTP, with proprietary Microsoft extensions, is found in most Microsoft Windows operating systems. Thus, it is an

attractive and widely accessible vehicle for the creation of VPNs. However, there has been criticism levied at the underlying security of Microsoft's original PPTP implementation and the improved version.

Some VPN clients use proprietary technologies. In a number of cases, a single VPN client allows the user to choose between a proprietary VPN scheme and a standardized one. Proprietary schemes restrict the user to a particular vendor's VPN products, and should be avoided wherever possible. Standardized schemes also have the advantage of security analysis and testing performed by a wider community of users and analysts.

7.4   Peer authentication

Before a telecommuter can conduct VPN-secured communications, each party involved in the communication must verify its identity with the other party. This ensures that not only are the communications protected, but that they are being conducted with a known and provably identifiable peer. The most common methods of peer authentication are:

- **Public key certificate**: A security gateway will generally possess its own public key certificate. A telecommuter will also have a certificate issued by an authority recognized by the security gateway. When a user attempts to make a connection to the VPN through the security gateway, the gateway will present the user (in reality the VPN software on the user's computer) with its certificate that will be checked to ensure that the gateway is correct (to avoid spoofing attacks). Next the security gateway will require a certificate from the user (again the VPN software on the user's computer generally performs this step) to ensure that the user has authorized access. Once the user is authorized the VPN connection will be initiated. This is a very secure method of authentication.

- **One-time password**: This is a password that is changed after each use; it is useful when the password is not adequately protected from compromise during login (e.g., the password is transmitted over an insecure network). Under this approach, each user is given a password generator that looks much like a pocket calculator or a software program that can generate the passwords. The user enters a PIN to activate the password generator; the password generator creates a random password (or number sequence) using a procedure that is duplicated at the central system. The user will then enter the generated password in the VPN software on his/her machine that will in turn forward it to the security gateway. If the password generated by the user and the security gateway match, the user is authorized to use the VPN. If the password is intercepted, an intruder could not use it for later access because it is valid only for this one session.

- **Password**:   A password is a protected or private character string used to authenticate and identify. Generally, a password is encrypted during transmission for protection. When authenticating to a security gateway the user enters his/her password. The VPN client then generates an encrypted hash of the password and sends it to the gateway. The security gateway then compares the hash to the one it has on file for the user. If the two match, the user is authenticated and connected to the VPN.

7.5   Policy configuration

The fortunate telecommuter will obtain a VPN client that has been pre-configured to satisfy the employer's security policies. If that is not the case, the VPN client will need to be configured with security protections that satisfy the employer's security requirements.

Many VPN clients will allow VPN-secured traffic to be either encrypted or integrity-protected, without requiring both types of protection. For a truly secure VPN, both encryption and integrity protection should be applied. Without encryption, unauthorized parties can read the traffic. Without integrity protection, encrypted traffic is susceptible to attacks that can result in unauthorized modification of the message.

Some of the policy-related choices are:

- **Encryption algorithm**: Triple DES (Data Encryption Standard) is the encryption algorithm that is most commonly used today. NIST's AES (Advanced Encryption Standard) has been approved, and will most likely replace triple DES as the default VPN encryption algorithm. Many VPN clients are configured with DES as the default encryption algorithm; AES or triple DES are preferable to DES, since traffic using DES for encryption could be decrypted (although only with sophisticated hardware and software) by parties other than the intended recipient.

- **MAC (message authentication code) algorithm**: HMAC-SHA-1 is the national standard message authentication algorithm.   HMAC-MD5 is also usable for today's VPNs.

- **Selective or total protection**: Most VPN clients will allow either some or all of the traffic to be protected.

7.6   VPN operation

The following are necessary steps to create a VPN:

1. Install the VPN client.

2. Obtain the required public key certificates, password(s), and/or one-time password generator. If all protected communications will be handled by the gateway, no other peer credentials are required. However, if the telecommuter will be conducting peer-to-peer VPN communications, credentials valid for those peers will be required as well. They can be obtained beforehand or exchanged in the course of the VPN negotiations. If the latter method will be used, it is important to ensure that the VPN client can dynamically request and process these credentials.

3. Configure the VPN client.

4. Put the VPN client into "operational" mode.

5. Perform a trial run. A number of VPN clients have a of "test" button that will do this. It is important to ensure that, after VPN client installation and configuration, both outbound and inbound communications can still take place successfully. It is

also a good idea to try to send and receive some unauthorized traffic, to ensure that unprotected communications are unsuccessful.

7.7   Summary Recommendations

A virtual private network (VPN) serves as an encrypted "tunnel" between two organizations (or hosts) that makes it possible for secured communication to occur over public networks. This tunnel allows a variety of different types of traffic, rather than a single encrypted connection such as an e-commerce credit card transaction using a web server. To ensure correct operation, the VPN must be carefully configured on both the organization's central office systems and the telecommuter's remote system. Users should also be educated on VPN operation, since current implementations are not as simple or "transparent" as some other security applications. Organizations considering a VPN should thus proceed with caution, first ensuring that security goals cannot be achieved with less complex mechanisms. If a VPN is used, the organization's system administrators should be responsible for correctly configuring the VPN, and for providing telecommuters with properly configured software for their offsite systems.

8   Telecommuting Architectures

Telecommuting can be approached in a number of ways, with a variety of tradeoffs between security and convenience. The appropriate choice for a user and organization depends on requirements for the tasks conducted by the user away from the office. From a security standpoint, the guiding principle to keep in mind is "least privilege". That is, privileges accorded to users should be the minimum necessary to do their jobs. Even if fully trusted, users who have excessive privileges may accidentally misuse them, leading to problems in the organization's database or daily operations, or intruders who compromise user accounts may deliberately use the excessive privileges to cause even greater damage. This section discusses some approaches to three components of telecommuting – voice communication, electronic mail, document and data exchange - with advantages and disadvantages of each.

8.1   Voice Communication

Depending on the sensitivity of communications between the offsite and main offices, telephone security may be a consideration. The variety of choices for telephones that has developed over the past decade spans a wide spectrum of privacy capabilities. At the low end are ordinary cordless phones, whose calls may be picked up by walkie-talkies, baby monitors, and radio scanners. The most secure home-use telephones are traditional corded models, but there are a number of other options, summarized below.
Note: classified discussions are not permitted on any of the equipment discussed here. Any of the telephones discussed in this section can be attacked by a knowledgeable adversary. This discussion is provided simply to distinguish between those systems that require special knowledge and those that are vulnerable to casual scanning.

Cordless, 46 – 47 MHz. These commonplace cordless models are the most widely used among portable home phones. They are easily intercepted, and should be regarded as providing no security at all. Some models provide a "privacy" or "scrambler" feature based on audio frequency inversion. While this feature requires special equipment to defeat, the necessary equipment is easy to build, and plans are available on the Internet, so these phones should not be considered secure.

Cordless, 900 MHz. These high-end phones are not as susceptible to eavesdropping as ordinary cordless models, but they can be picked up using some radio equipment. Some models employ "frequency hopping" or spread spectrum technology, which uses a rapidly changing set of frequencies to scramble transmissions. Models that provide spread spectrum are reasonably secure for most unclassified uses.

Cordless, 2.7 GHz. These newer models are, like 900 MHz models, less likely to be intercepted than ordinary cordless phones, but should be considered secure for most unclassified use only if they provide spread spectrum.

Cell phones. The most widely used cellular telephones operate on frequencies around 800 MHz, which fall within the UHF television band. Radio scanners and television sets with UHF dial tuners can intercept cell phone conversations, so these telephones are no more secure than ordinary cordless models.

Digital PCS.   Some newer mobile phones use digital technology. These systems are more difficult to intercept than ordinary cell phones, and are probably adequately secure for most unclassified uses.

Corded telephones.   Physical connections are required to intercept traditional corded telephones, so they are reasonably secure for most unclassified use.

PC based voice communication (Voice over IP).   Within the past few years, a number of services have begun offering telephone calls, including long distance, over the Internet. Known as "voice over IP" (VOIP), the services convert speech to Internet messages and transmit them to a facility that interfaces with the telephone network. Any PC can become a telephone with the addition of a microphone and special software to access the service. The party on the other end is normally not required to have a PC to receive the call; the services connect calls directly with ordinary telephones on the receiving end. From a security standpoint, this type of connection is only as secure as the weakest link in the chain from the user's PC, to the Internet service provider, through various Internet nodes, and eventually to the telephone network. Because of the potential for vulnerabilities in one or more of the Internet components, VOIP should not be considered secure unless some form of encryption is used.

8.2   Electronic Mail

Most workers need to be able to send and receive e-mail at either their main office or offsite.   E-mail can be handled in a number of ways, with varying security considerations. Some approaches can affect the vulnerability of main office systems

Remote login. The most common method of receiving e-mail offsite is to have the telecommuter log in remotely and receive e-mail messages from a central server just as at the office. This approach requires the organization to be especially careful in password management and in blocking access between mail servers and other critical organization computers. If several hundred users have remote login access, there is a significant chance that a few will be careless with passwords, making it possible for intruders to gain at least some access to the e-mail server. Also note that many remote e-mail tools use the POP3 protocol, so passwords may be sent unencrypted.

E-mail forwarding. One simple approach is to set up the e-mail system on the user's main office computer to automatically forward a copy of each e-mail received to the user's ISP account. Although this method does not protect the privacy of messages through encryption, as a VPN would, it avoids the need for users to log in to a computer at the main office. This option may be appropriate if privacy of e-mail messages is not a significant concern, but the organization wants to minimize the chance that an intruder could gain access to main office systems by compromising a user's offsite computer.

Virtual Private Network (VPN).   A VPN uses encryption methods to provide secure communication between offices. Properly implemented, a VPN can provide a high degree of security. E-mail and other traffic will be encrypted, minimizing the risk to privacy. However, the offsite computer, especially if it has a full-time connection to the Internet, may be left open to intruders if not configured properly. Use of a VPN does not obviate the need for normal precautions. For example, a worm or virus sent by e-mail over a VPN can infect the user's computer, leaving open a back door for intruders to exploit, or damaging files.

8.3   Document and Data Exchange

In addition to e-mail, almost all users will have a need to move some data files between main and offsite computers. Files may be documents, spreadsheets, database entries, or in some cases, graphics, audio, and video. Users also vary in how frequently they need access to files. The frequency and type of data exchange required by a user's job are considerations in making tradeoffs between convenience and security for data exchange.

Remote connection. Some users need offsite access to most or all of the files on their office systems. For example, a tax consultant or lawyer with a large number of clients may receive calls at any time from clients requesting help.   Popular software packages such as "PC Anywhere" allow partial or complete access to the main office computer from offsite. The tradeoff for this convenience is that configuring an office system for remote access may make it easy for intruders to break in. Hacking sites distribute methods and tools for breaking in to remote connection packages.   If remote access is needed, system administrators should provide users with VPN tools and encryption software.

FTP and web file transfer. The File Transfer Protocol (FTP) is an Internet standard for transmitting files between computers. It can be used either as a stand-alone tool, or as is becoming more common today, embedded in web sites set up for uploading and downloading files. Like remote connection tools, FTP can leave systems vulnerable if not properly configured and operated. At the server end, FTP should be configured to limit access to only those directories or folders that are essential; avoid providing access to the entire PC. As with remote access tools, strong authentication and passwords are needed for users.

E-mailing document and data files. Some users work with only a few documents or files at a time. For example, a researcher or technical writer may have a small number of projects over the course of several months. These users can e-mail documents and files between their office and offsite e-mail addresses, as long as they are careful to send the latest copy of a file after completing work on it for the day. This arrangement avoids the need to make office PCs accessible from outside the organization firewall, denying a significant path of entry to intruders.

Virtual Private Network (VPN) A VPN uses encryption methods to provide secure communication between offices. Properly implemented, a VPN can provide a high degree of security.   E-mail and other traffic will be encrypted, minimizing the risk to privacy. However, the offsite computer, especially if it has a full-time connection to the Internet, may be left open to intruders if not configured properly. Use of a VPN does not obviate the need for normal precautions. For example, a worm or virus sent by e-mail over a VPN can infect the user's computer, leaving open a back door for intruders to exploit, or damaging files.

Physical transfer.   Laptop computers today have such high performance and data capacity that many workers can keep all their documents and files on a laptop and use it as their primary computer at either main or offsite office. This arrangement avoids the need for most electronic transmission of documents, at the cost of requiring diligence in backups and, in some cases, encryption of data on the computer, since the laptop may be stolen. Another drawback to this approach is that viruses or other malicious software that makes its way onto the home system may contaminate the corporate network, so users must be especially software to apply virus checkers to files on their home systems.

	Security (for unclassified use)			Administrative Complexity
	Confidentiality	Integrity	Availability	
Voice Communication				
Cordless	Poor	N/A	Good	Good
Cordless, with spread spectrum	Good	N/A	Good	Good
Cellular	Poor	N/A	Good	Good
Digital PCS	Good	N/A	Good	Good
PC phone	Fair	Fair	Fair	Fair
Corded phone	Good	N/A	Good	Good
Electronic Mail				
Remote login	Fair (good w/ encryption)	Fair	Good	Good (fair w/ encryption)
E-mail forwarding	Fair (good w/ encryption)	Good	Good	Good (fair w/ encryption)
Virtual Private Network (VPN)	Good	Good	Good	Fair
Document and Data Exchange				
Remote connection	Fair (good w/ encryption)	Fair	Good	Good (fair w/ encryption)
FTP and web file transfer	Fair (good w/ encryption)	Good	Good	Good (fair w/ encryption)
E-mail	Fair (good w/ encryption)	Good	Good	Good (fair w/ encryption)
Virtual Private Network (VPN)	Good	Good	Good	Fair
Physical	Good	Good	Good	Fair

Table 8. Alternatives for voice, e-mail and file transfer.

8.4 Selecting Components

Table 8 summarizes security features of choices for voice communication, e-mail, and document and file transfer. Choices should be based on the organization's needs, but they can be loosely grouped into three architectures - Disconnected, Remote Access, and Integrated – reflecting the degree to which the offsite system is coupled to the main office system. Tighter coupling generally means more convenience, at the cost of greater administrative complexity.

8.4.1 Disconnected

Users who do not need daily interaction with the agency's systems or database may be able to telecommute successfully using only e-mail and telephone contact with the office.

For example, a user who telecommutes or two days a week, and whose job consists largely of writing and document preparation, may never need to log in to agency systems from a remote location. Provided that they are not sensitive, documents can be e-mailed back and forth between the agency system and the user's ISP e-mail account, or simply carried by the user on physical media (e.g., on a laptop computer). As a result, users never need to log in to a system at the main office.

This approach minimizes vulnerabilities at the main office, by eliminating the need for outside access, but clearly is not suitable for users who need to operate sophisticated applications across the network securely. In addition, it relies on security at the user's ISP to protect e-mail confidentiality.

- Best suited to users who require little computer interaction with office.
- All communication between office and remote location is by e-mail and telephone.

8.4.2   Remote Access

When users need to access a large number of files on the main office computer, it may be necessary to allow for remote logins from the offsite computer. In this case, strong authentication should be used if possible, to minimize the vulnerabilities in providing external access.

- For users who need to access wide variety of files at main office from offsite.
- Allows remote login for file transfer, but not for complex applications (e.g., accounting or transaction processing) across the network.

8.4.3   Integrated

A virtual private network can provide a high level of security and convenience for the user. Encryption protects all interaction between the offsite computer and the main office, so that in many ways the user's offsite computer is as secure as one on the main office local network. This approach makes it possible to allow offsite users to operate applications such as scheduling, budget analysis, or other complex systems from the remote site. The tradeoff for a VPN is in cost and complexity of administration. Note also that operating a VPN does not guarantee protection from viruses and e-mail worms.
- For users who need to operate complex applications across the network.
- Better security but greater expense.

Table 9 summarizes these three architectures.

Table 9. Summary of telecommuting architectures

Architecture	Components	Issues
Disconnected	E-mail access through forwarding, file transfer by e-mail or physical	• Relies on security at ISP • Strong authentication probably not available • Requires automatic forwarding of e-mail from office
Remote access	E-mail access through remote login, file transfer by remote access or web/FTP	• Relies on security at agency e-mail gateway • Allows for strong authentication (biometrics, one-time passwords)
Integrated	E-mail and file transfer through VPN service	• VPN required • More expensive

8.5   Summary Recommendations

Federal agencies should provide telecommuting users with guidance on selecting appropriate technologies, software, and tools that are consistent with the agency network and with agency security policies. Users have a wide variety of approaches to choose from in establishing an off-site office. Sophisticated technologies such as virtual private networks can provide a high level of security, but are more expensive and complex to implement than other solutions. Many users, particularly if they do not require interactive access to agency databases, can be afforded with an adequate degree of security at very low cost and with little additional software, easing burdens on both the user and system administrators at the central computing system.

9   Agency/Enterprise Considerations for Telecommuting Security

Organizations supporting telecommuting need to establish and follow a reasonable and consistent security policy for their users. Ideally, the organization should provide the telecommuter with a home system that is configured using the same policy and guidelines that are employed for employees in the office.   Policies will vary according to organizational needs, but some basic policy features are common to most organizations. This section describes some fundamental considerations for a telecommuting security policy that can be used as a basis for a document tailored to organizational needs. Refer to previous sections of this publication for details on the technologies discussed in this section.

9.1   Controlling System Access

If users need to log in remotely to internal systems, ensure that login process uses an appropriately strong mechanism to validate a user's identity.   In some cases, a user ID/password combination may be adequate, if passwords are sufficiently strong (see instructions below for creating strong passwords). For example, if the user only logs into the internal system to retrieve non-sensitive information, relatively little damage is done if the password is compromised.   In most cases, though, a stronger mechanism will be required. There are three methods of authenticating users:

1.   What they know (e.g., user id, password, personal identification number [PIN])

2.   What they have (e.g., smartcard or one-time password generator)

3.   What they are (e.g., retina pattern, or hand geometry).

The strongest authentication mechanisms usually employ more than one of the above authentication methods. For example, smartcards are really a two-factor authentication scheme that allow access based on what a user knows (the password required to access the smartcard) and what the user has (the smartcard). Authentication options include:

Strong passwords. Password cracking programs are widely available on the Internet. Cracking programs use a dictionary of thousands of words and names, seeking to find one that the user has selected for a password.   Dictionaries of 500,000 passwords are reported, and an intruder can try all of them in an overnight run.   Common names of people or pets are the first passwords tried, because they are frequently used as passwords. Ordinary words are tried next, followed by words and names with one or two digits tacked on at the end. Use at least eight characters, including two or more digits. and characters. Digits and characters should be placed in random positions between letters, not just at the beginning or end.   Also password crackers will attempt common substitutions of numbers and characters for letters (e.g., h4ckm3 for hackme, r@ts for rats, p001 for pool, etc.).

One-time password generators. With this system, each user is given a password generator that looks much like a pocket calculator. To access the central system, the user enters a PIN on the password generator to gain access to it; the password generator creates a random password (or number sequence) using a procedure that is duplicated at the central system. If the password is intercepted, an intruder could not use it for later access because it is valid only for one session.

Smartcards. Smartcard access control is similar to the one-time password generator approach, except that the smart card, which contains a microprocessor, automates most of the login process. The user gains access to the smartcard using a password or PIN, then the card does the rest. A drawback to this approach is that the user's computer must have a smartcard reader attached to it.

Biometrics. Identifies and authenticates users based on what they are. Some biometric characteristics currently used in commercial products are fingerprints, hand geometry, voice pattern, retinal pattern, iris pattern, and handwriting dynamics. Currently biometric products are relatively more expensive than other mechanisms, although prices are declining as they gain popularity. Another drawback to biometrics is that they require a special device attached to the user's computer.

9.2 Protecting Internal Systems

Restricted Access. Access privileges should be implemented at the minimum level required (i.e., deny access to all systems, then allow access to only those required and at the minimum level required). The level of access may differ when telecommuting than when at the normal duty station. Determine the specific systems to which the user requires access from remote locations. Finally, the employee's supervisor should confirm, in writing, that the employee requires not only remote access, but also access to the specific systems identified to perform their work assignments.

Firewalls and Secure Gateways. A secure gateway or firewall blocks or filters access between two networks, often between an internal trusted network and an external untrusted (public) network such as the Internet. For telecommuting, organizations should determine what systems and information to make available to telecommuters using public networks for remote access; what level of protection is needed to ensure that only authorized users can access the internal network; and how to ensure that the gateway or firewall is functioning properly. For more information on selecting and installing firewalls, see

☼ NIST Draft Special Publication: "Guide to Firewall Selection and Policy Recommendations" , October, 2001.
PDF: http://csrc.nist.gov/publications/drafts/Firewall-Guide.pdf

☼ NIST Special Publication SP 800-10 "Keeping Your Site Comfortably Secure: An Introduction to Internet Firewalls", December 1994.
PDF: http://csrc.nist.gov/publications/nistpubs/800-9/800-9.pdf
Compressed ZIP: http://csrc.nist.gov/publications/nistpubs/800-9/800-9SP.zip

Location of Resources. If possible, resources needed by telecommuters should be placed in a DMZ[22] in order to better control access to the internal network. This may be a feasible alternative to avoid direct access to the internal network by telecommuters. However, this may not be possible for sensitive information.

---

[22] A demilitarized zone (DMZ) is a networking term for a sub-network that is behind an organization's firewall but not part of the main network. The primary purpose of a DMZ is to isolate those machines that need to be accessible from outside the organization's network in order to limit the exposure of the internal network while still providing some level of protection to the exposed machines.

Proxy servers. Most telecommuting employees require less access than when working at their central office. Traveling employees may require access only to electronic mail. There are many firewall implementations that use an electronic mail proxy to allow access to the files on a protected system without having to directly access that system. However, some telecommuting employees need access to internal resources. In this case, a more secure solution, such as a VPN, should be used.

Secure Gateways. A secure gateway, or series of gateways, can be used to divide internal resources based on access needs of telecommuters. For example, computers with high-risk organizational data (such as proprietary business plans) may be separated by a gateway from systems with a lower level of risk. A series of gateways can be used to further restrict access to the highest-risk systems. For some situations, current firewall technology can be used to give virtual access by using proxies. In addition, current firewalls can use filtering to limit access to certain types of resources. For many organizations, the primary security function of the secure gateway is to provide robust authentication of users. Secure gateways may also provide additional auditing and session monitoring, and intrusion detection.

Encryption. If a telecommuting employee is transferring data that an eavesdropper would want, encryption may be necessary. Software- or hardware-based encryption provides strong protection against electronic eavesdropping. Use of encryption is required when sensitive unclassified information is transmitted over an untrusted public network domain (e.g. the Internet). Since employees do not always know when they are in a high-threat area, management must train employees to consider this potential threat.

Telecommuting Center Controls. At a minimum, organizations should require robust authentication from telecommuting centers. If communications encryption is supported by the center, organizations should be aware that data might not be encrypted while it is inside the center. The encryption may occur at the point prior to where data enters the public network and thus the data is subject to the interception while on the telecommuting center's network.

9.3   Protecting Home Systems

Organizations may implement several countermeasures to ensure protection of Government information assets when an employee telecommutes from his or her home.

Security Policy. Organizations should implement a security policy for their specific telecommuting environment. Rules should define the specific reasons, expectations, and benefits of telecommuting within their organization. Individuals must demonstrate an understanding of the standards of care and the importance of having protective measures to ensure the availability, integrity, and confidentiality of the data they will be processing. If the telecommuter is to be accessing, processing, or storing sensitive unclassified information specific rules must be established for that situation.

Employee Accountability. Employees should sign an acknowledgment of the conditions for use of the telecommuting environment. The acknowledgment should also be endorsed by the employee's supervisor to ensure proper authorization for remote access.

Removable Hard Drives. If data is stored on a removable hard drive (or floppy) and the media device can be separately secured, the risk of data compromise is greatly reduced.

Data Encryption. Data can be kept encrypted on the hard disk. This protects its confidentiality; and some technologies may help in the detection of attempts to change files.

Dedicated Use. If an organization requires dedicated system use (i.e., the system will only be used for specified Government access and processing), management should recognize that it is difficult to enforce. It should be assumed that at some point the system is likely to be used by someone other than the employee. In addition, as home networks become commonplace, it is likely that non-employees may have access to the system through the home network.

Locked Rooms or Storage Containers. It is necessary to provide physical security to systems and data against the threat of unauthorized disclosure, destruction, alteration, or theft.

Home System Availability. In addition to the possibility of failure or theft of a home computer, it may not be compatible with office configurations. For example, the home computer may use a different operating system. This and other circumstances may complicate configuration, software support, troubleshooting, or repair. Organizations should ensure that policies are in place to cover all of these situations. Hand receipts, or property passes, should be required for all government hardware and approved licensed software that is taken home by an employee.

This section is adapted from Department of Energy publication.

The following definitions highlight important concepts used in this document.

802.11
In wireless LAN (WLAN) technology, 802.11 refers to a family of specifications developed by a working group of the Institute of Electrical and Electronics Engineers (IEEE). There are three specifications in the family: 802.11, 802.11a, and 802.11b. All three specify the use of CSMA/CA (carrier sense multiple access with collision avoidance) as the path-sharing protocol. The 802.11 and 802.11b specifications apply to wireless Ethernet LANs, and operate at frequencies in the 2.4-GHz region of the radio spectrum. Data speeds are generally 1 Mbps or 2 Mbps for 802.11, and 5.5 Mbps or 11 Mbps for 802.11b, although speeds up to about 20 Mbps are realizable with 802.11b. The 802.11b standard is backward compatible with 802.11.The 802.11a specification applies to wireless Asynchronous Transfer Mode (ATM) systems and operates at radio frequencies between 5 GHz and 6 GHz. A modulation scheme known as OFDM (orthogonal frequency-division multiplexing) makes possible data speeds as high as 54 Mbps, but most commonly, communications takes place at 6 Mbps, 12 Mbps, or 24 Mbps.

Active Content
Active content refers to electronic documents that are able to automatically carry out or trigger actions at a computer platform without the intervention of a user.

ActiveX
A loosely defined set of technologies developed by Microsoft. ActiveX is an outgrowth of two other Microsoft technologies called OLE (Object Linking and Embedding) and COM (Component Object Model). As a moniker, ActiveX can be very confusing because it applies to a whole set of COM-based technologies. Most people, however, think only of ActiveX controls, which represent a specific way of implementing ActiveX technologies.

Advanced Encryption Standard
The Advanced Encryption Standard (AES) specifies a US Government-approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information. Encryption converts data to an unintelligible form called ciphertext; decrypting the ciphertext converts the data back into its original form, called plaintext. The AES algorithm is capable of using cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt data in blocks of 128 bits.

The National Institute of Standards and Technology (NIST) selected the algorithm, called Rijndael (pronounced "Rhine Doll") in an international public competition. Rijndael was developed by Belgian cryptographers Joan Daemen and Vincent Rijmen.

Broadband
Broadband refers to telecommunication in which a wide band of frequencies is available to transmit information. Because a wide band of frequencies is available, information can be multiplexed and sent on many different frequencies or channels within the band concurrently, allowing more information to be transmitted in a given amount of time (much as more lanes on a highway allow more cars to travel on it at the same time).

Boot-Sector Viruses

Boot-sector viruses locate themselves in a specific part of the hard disk or floppy disk called the boot sector. Thus they are loaded in to memory when the computer first boots up. Once in memory, the boot-sector viruses can infect any hard disk and floppy accessed by the user. With the advent of more modern operating systems and a great reduction in users sharing floppies there has been a major reduction in this type of virus. These are now relatively uncommon.

Cable Modem

A cable modem is a device that enables a user to hook up their PC to a local cable television line and receive data at about 1.5 Mbps. This data rate far exceeds that of the prevalent 28.8 and 56 Kbps telephone modems and the up to 128 Kbps of Integrated Services Digital Network (ISDN) and is above the data rate available to most subscribers of Digital Subscriber Line (DSL) telephone service. A cable modem has two connections: one to the cable wall outlet and the other to a PC or to a set-top box for a TV set. Although a cable modem does modulation between analog and digital signals, it is a much more complex device than a telephone modem. It can be an external device or it can be integrated within a computer or set-top box. Typically, the cable modem attaches to a standard 10BASE-T Ethernet card in the computer.

Computer Virus

A computer virus is similar to a Trojan horse insofar as it is a program that contains hidden code, which usually performs some unwanted function as a side effect. The main difference is that the hidden code in a computer virus can only replicate by attaching a copy of itself to other programs and may also include an additional "payload" that triggers when specific conditions are met. See entries for **Boot Sector Virus**, **File Infector Virus** and **Macro Virus**.

Cookie

A piece of state information supplied by a Web server to a browser, along with a requested resource, for the browser to store temporarily and return to the server on any subsequent visits or requests.

Data Encryption Standard (DES)

Data Encryption Standard (DES) is a US Government-approved encryption algorithm used by business and civilian government agencies. The Advanced Encryption Standard (AES) is designed to replace DES. The original "single" DES algorithm is no longer secure because it is now possible to try every possible key with special purpose equipment or a high performance cluster. Triple DES (see glossary entry below), however, is still quite secure.

Digital Subscriber Line (DSL)

DSL (Digital Subscriber Line) is a technology for bringing high-bandwidth information to homes and small businesses over ordinary copper telephone lines. xDSL refers to different variations of DSL, such as ADSL, HDSL, and RADSL. The variation support data at rates up to 6.1 Mbps (of a theoretical 8.448 Mbps), enabling continuous transmission of motion video, audio, and even 3-D effects. More typically, individual connections provide from 1.544 Mbps to 512 Kbps downstream and about 128 Kbps upstream. A DSL line can carry both data and voice signals and the data part of the line is continuously connected.

Encryption

Encryption is the conversion of data into a form, called a ciphertext, that cannot be easily understood by unauthorized people. Decryption is the process of converting encrypted data back into its original form, so it can be understood. The use of encryption/decryption

is as old as the art of communication. A cipher, often incorrectly called a "code," can be employed to keep unauthorized parties from obtaining the contents of transmissions. (Technically, a code is a means of representing a signal without the intent of keeping it secret; examples are Morse code and ASCII.)

Simple ciphers include the substitution of letters for numbers, the rotation of letters in the alphabet, and the "scrambling" of voice signals by inverting the sideband frequencies. More complex ciphers work according to sophisticated computer algorithms that rearrange the data bits in digital signals.

In order to easily recover the contents of an encrypted signal, the correct decryption key is required. The key is an algorithm that "undoes" the work of the encryption algorithm. Alternatively, a computer can be used in an attempt to "break" the cipher. The more complex the encryption algorithm, the more difficult it becomes to eavesdrop on the communications without access to the key.

Ethernet
Ethernet is the most widely installed local area network (LAN) technology. Specified in a standard, IEEE 802.3, Ethernet was originally developed by Xerox and then developed further by Xerox, DEC, and Intel. An Ethernet LAN typically uses coaxial cable or special grades of twisted pair wires. The most commonly installed Ethernet systems are called 10BASE-T and 100BASE-T and provide transmission speeds up to 100 Mbps.

File Infector Virus
File infectors are viruses that work by attaching themselves to program files, such as word processors and computer games. When the user runs an infected program, the virus adds itself to the computer memory so that it can infect other programs the user runs. Were most common type of virus but are nearly "extinct" due to changes in operating system design.

Firewall
A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

Interpreter
An interpreter is a program that processes a script or other program expression and carries out the requested action, in accordance with the language definition.

IP address
An IP address is a unique number for a computer that is used to determine where messages transmitted on the Internet should be delivered. The IP address is analogous to a house number for ordinary postal mail.

IPSEC
A protocol that provides security capabilities at the Internet Protocol (IP) layer of communications. IPsec's key management protocol, the Internet Key Exchange (IKE), is used to negotiate the secret keys that protect VPN communications, and the level and type of security protections that will characterize the VPN.

Java

Java is an object-oriented language similar to C++, but simplified to eliminate language features that cause common programming errors. Java source code files (files with a .java extension) are compiled into a format called bytecode (files with a .class extension), which can then be executed by a Java interpreter. Compiled Java code can run on most computers because Java interpreters and runtime environments, known as Java Virtual Machines (VMs), exist for most operating systems, including UNIX, the Macintosh OS, and Windows. Bytecode can also be converted directly into machine language instructions by a just-in-time compiler (JIT).

JavaScript

A scripting language developed by Netscape to enable Web authors to design interactive sites. Although it shares many of the features and structures of the full Java language, it was developed independently. JavaScript can interact with HTML source code, enabling Web authors to spice up their sites with dynamic content. JavaScript is endorsed by a number of software companies and is an open language that anyone can use without purchasing a license. Recent browsers from Netscape and Microsoft support it, though Internet Explorer supports only a subset, which Microsoft calls Jscript.

Local Area Network (LAN)

A Local Area Network is a computer network that spans a relatively small area. Most LANs are confined to a single building or group of buildings. However, one LAN can be connected to other LANs over any distance via telephone lines and radio waves. A system of LANs connected in this way is called a wide-area network (WAN).

Macro Virus

A type of computer virus that is encoded as a macro embedded in a document and executes when the document is opened. Many desktop applications, such as word processors and spreadsheets, support powerful macro languages and are thus susceptible to this type of virus.

Malicious Code

Malicious code refers to programs that are written intentionally to carry out annoying or harmful actions. They often masquerade as useful programs or are embedded into useful programs, so that users are induced into activating them. Types of malicious code include Trojan horses, computer viruses, and worms.

Malicious Mobile Code

Malicious mobile code is a relatively recent development that has grown with the increased use of Web browsers. Mobile code is used by many Web sites to add functionality and is legitimate and includes ActiveX, JavaScript, and Java. Unfortunately, although it was initially designed to be secure, mobile code has vulnerabilities that allow entities to create malicious programs. A user can infect his/her computer with malicious mobile code (e.g., a Trojan horse program that transmits information from the user's PC) just by visiting a Web site.

Operating System

An operating system (sometimes abbreviated as "OS") is the program that, after being initially loaded into the computer by a boot program, manages all the other programs in a computer. The other programs are called applications or application programs. The application programs make use of the operating system by making requests for services through a defined application program interface (API). In addition, users can interact

directly with the operating system through a user interface such as a command language or a graphical user interface (GUI).

Proxy Server
A server that sits between a client application, such as a Web browser, and a real server. It intercepts all requests to the real server to see if it can fulfill the requests itself. If not, it forwards the request to the real server.

Public Key Certificate
An identifying digital certificate that typically includes the public key, information about the identity of the party holding the corresponding private key, and the operational period for the certificate, authenticated by the digital signature of the certification authority (CA) that issued the certificate. In addition, the certificate may contain other information about the signing party or information about the recommended uses for the public key. A subscriber is an individual or business entity that has contracted with a CA to receive a digital certificate verifying an identity for digitally signing electronic messages.

Public (Asymmetric) Key Encryption
Public key cryptography uses "key pairs," a private key and a mathematically related private key. Given the public key it is infeasible to find the private key. The private key is kept secret while the public key may be shared with others. A message encrypted with the public key can only be decrypted with the private key. A message can be digitally signed with the private keys and anyone can verify the signature with the public key.

Plugin
A plugin is a software module that adds a specific feature or service to an application. The most common examples are the plug-ins available for Web browsers that enable them to display different types of audio or video messages.

Script
A script is a sequence of commands, often residing in an ASCII file, which can be interpreted and executed automatically. Unlike compiled programs, which execute directly on a computer processor, a script must be processed by another program that carries out the indicated action.

Scripting Language
A scripting language defines the syntax and semantics for writing scripts. Typically, scripting languages follow the conventions of a simple programming language, but they can also take on a more basic form such as a macro or a batch file. Javascript, VBScript, and Perl are examples of scripting languages.

Secret (Symmetric) Key Encryption
This is the traditional method used for encryption. The same key is used for encryption/decryption and is known only to the party or parties that exchange secret messages. The biggest problem with symmetric key encryption is securely distributing the keys. Public key techniques are now often used to distribute the symmetric keys.

Secure Socket Layer (SSL)
Secure Sockets Layer, a protocol developed by Netscape for transmitting private documents via the Internet. SSL works by using a public key to encrypt data that's transferred over the SSL connection. Both Netscape Navigator and Internet Explorer support SSL, and many Web sites use the protocol to obtain confidential user information, such as credit card numbers. By convention, URLs that require an SSL connection start with "https:" instead of "http:."

SHA-1

The Secure Hash Algorithm (SHA-1) specified in FIPS 180-1, *Secure Hash Standard* (SHS), is for computing a condensed representation, called a "message digest", of a message or a data file. SHA-1 is currently the only FIPS-approved method for secure hashing. However, NIST expects to add new, larger hash algorithms to provide a suite of cryptographic hash algorithms of comparable strength to the AES.

Spyware

Spyware is a program included with an application that communicates with its home site unbeknownst to the user. Spyware programs have been discovered with many shareware or freeware programs and even some commercial products. Notification of this hidden functionality either may not at all or occur somewhere in the license agreement. News reports have accused various spyware programs of inventorying software on the user's system, collecting or searching out private information, and then periodically shipping the information back to the home site.

TCP/IP

Transmission Control Protocol/Internet Protocol, the protocol suite used by the Internet. A protocol suite is the set of message types, their formats, and the rules that control how messages are processed by computers on the network.

Triple DES

An implementation of the Data Encryption Standard (DES) algorithm that uses three passes of the DES algorithm instead of one as used in ordinary DES applications. Triple DES provides much stronger encryption than ordinary DES, requiring approximately 67 million times as much effort to break, but it is less secure than AES.

Trojan Horse (a.k.a. Trojan)

A Trojan horse is a useful or seemingly useful program that contains hidden code of a malicious nature. When the program is invoked, so is the undesired function whose effects may not become immediately obvious. The name stems from an ancient exploit of invaders' gaining entry to the city of Troy by concealing themselves in the body of a hollow wooden horse, presumed to be left behind by the invaders as a gift to the city.

Update (Patch)

An update (sometimes called a "patch") is a "repair" for a piece of software (application or operating system). During a piece of software's life, problems (called bugs) will almost invariably be found. A patch is the immediate solution that is provided to users; it can sometimes be downloaded from the software vendor's Web site. The patch is not necessarily the best solution for the problem and the product developers often find a better solution to provide when they package the product for its next release.

A patch is usually developed and distributed as a replacement for or an insertion in compiled code (that is, in a binary file or object module). In larger operating systems, a special program is provided to manage and keep track of the installation of patches.

Uniform Resource Locator (URL)

Uniform Resource Locator, the global address of documents and other resources on the World Wide Web. The first part of the address indicates what protocol to use, and the second part specifies the IP address or the domain name where the resource is located.

For example, the two URLs below point to two different files at the domain nist.gov. The first specifies an executable file that should be fetched using the FTP protocol; the second specifies a Web page that should be fetched using the HTTP (Web) protocol:

- ftp://www.nist.gov/stuff.exe

- http://www.nist.gov/index.html

Virtual Private Network (VPN)
A virtual private network is a network that is constructed by using public wires to connect nodes. For example, there are a number of systems that enable you to create networks using the Internet as the medium for transporting data. These systems use encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted.

Virus
See **Computer Virus**.

Warez
A term widely used by hackers to denote illegally copied and distributed commercial software from which all copy-protection has been removed. Warez often contains viruses, Trojans and other malicious code and thus is very risk to download and use (legal issues notwithstanding).

Web Browser
A browser refers to any collection of software that lets individuals view Web content, and includes the GUI, MIME helpers, Java Interpreter, and other similar program components.

Web Bug
Tiny images, invisible to a user, placed on Web sites in such a way that they allow third parties to track use of Web servers and collect information about the user, including IP address, Host name, browser type and version, operating system name and version, and Web browser cookie.

Wired Equivalent Privacy (WEP)
Wired Equivalent Privacy, a security protocol for wireless local area networks (WLANs) defined in the 802.11b standard. WEP was intended to provide the same level of security as that of a wired LAN. LANs are inherently more secure than WLANs because LANs have some or all of the network inside a building that can be protected from unauthorized access. WLANs, which are over radio waves, therefore are more vulnerable to tampering. WEP attempted to provide security by encrypting data over radio waves so that it is protected as it is transmitted from one end point to another. **Note:** WEP has been broken and does not provide an effective security service against a knowledgeable attacker. Software to break WEP is freely available on the Internet.

Wireless Local-Area Network (WLAN)
A type of local-area network that uses high-frequency radio waves rather than wires to communicate between nodes.

Worm
A worm is a self-replicating program. Unlike a virus, it is self-contained and does not require a host program to replicate or any user intervention. Worms commonly utilize network services to propagate onto other computer systems. Although nowadays worms are associated with malicious code, the concept [Sho83] was originally introduced in the context of building useful applications.

Appendix A. Security Checklists

Home Computer Security Checklist

Antivirus Software

- Antivirus application is installed and is configured to:
    - Start with the boot of the operating system
    - Run the background and automatically scan all incoming files
    - Enable Web browser protection, if available
    - Automatically update the virus signature database weekly
    - Attempt to recognize unknown viruses, if available.

Spyware Removal Tools

- Install and run a spyware removal tool to identify and eliminate (as appropriate) spyware.
- On a monthly basis update and run spyware removal tool, again eliminate discovered spyware if appropriate.

Firewall

- A firewall is an application that is employed to monitor and limit dangerous packets from entering a network, providing the capability to:
    - Log all suspicious traffic (this is generally true for default installs)
    - Examine log on a periodic basis
    - Block traffic to ports that support services that should not be accessible from the Internet (e.g., NetBIOS, Telnet, etc.)
    - Automatically lockout network access to the host when network connectivity is not required (e.g., when the screensaver activates or computer is inactive for a fixed period of time)
    - Notify the user when an application attempts to make an outbound connection
    - Medium to high level of security (e.g., "paranoia level").

Encryption Software

- Ensure that appropriate encryption software is being used.

Securing the Operating System

- Secure or disable file and printer sharing.
- Ensure that the latest operating system patches are installed.
- Turn your system off when it is not being used.

Securing Wireless Networks

- Place wireless base station away from outside walls in order to minimize transmission of data outside of building.
- User additional encryption beyond WEP (VPN. PGP, etc.).
- Enable 128 bit WEP encryption.
- Change SSID to a hard guess password.

- Enable additional authentication schemes supported by you wireless base station.
- Disable broadcasts of SSID in the wireless base station beacon message.
- Disable SNMP or change the SNMP community strings to a hard to guess password.
- Install personal firewall on all wireless clients.

Online Security Assessment

- An online security assessment has scanned the current configuration (including the firewall).
- All major vulnerabilities identified by the assessment have been corrected and confirmed by a rescan.

Securing Web Browsers

- Browser(s) configured to limit or disable plugins.
- Browser(s) configured to limit ActiveX, Java and JavaScript.

Laptop Security Checklist

The need for an explicit laptop security checklist can be illustrated by the fact that, according to Safeware Insurance in 1999, the number of laptop computers stolen outnumbered the number of desktop computers stolen by almost 12 to 1.

Review Home Computer Security Checklist

- Where applicable, all elements from the home computer security checklist presented previously should be applied to a laptop computer. (Not all elements from home computer security checklist may apply).

Encryption Software

- Although mentioned above in the home computer security checklist, encryption is vital for protecting sensitive information on a mobile computer. Operating system features such as encrypting file system (EFS) or even discretionary access control (DAC) permissions can provide valuable security for a laptop that is stolen.

- Third party software such as PGP, Norton Internet Security, can provide similar levels of protection for laptop data.

Physical Security

- Laptops that spend a majority of their time in two or fewer places should be physically secured with a cable lock

- Cable locks are widely available on the Internet and in computer retail stores

- Almost all major laptop brands contain slot to attach lock cable

- Those that do not can have lock cable glued on

Set BIOS Password

- Set BIOS password to prompt user every time laptop is powered up

- Check for BIOS updates at least twice a year (or more) to "flash" BIOS.

Use Non-descript carrying case

- Avoid unwanted attention leather briefcase or obvious laptop case can attract in public places, especially airports, and while on planes

- If traveling with confidential information, pack information or information backup in separate bag from laptop in case of theft.

Identify Laptop with contact information

- Many companies and individuals place decals or markings on the laptop case that are difficult to remove and if done so, indicate obvious tampering

- Record serial number and other identification information about laptop twice, and keep one copy at home or in the office in case of theft. This information can be helpful to authorities searching for the laptop.

Backup all personal data on a regular basis

- In the event that your laptop does get stolen, all of your work is essentially useless without a backup of all of your personal data.

Consider purchasing advanced security features

- Should your computing needs or data security warrant it, products that offer increasingly advanced security features such as biometric login, motion sensing, "Lo-Jack" type location tracking are becoming increasingly cheaper to purchase for laptops.

- Software developers are responding to this demand by integrating these new technologies into common tasks of computer usage such as seamlessly logging in to the operating system.

Telecommuting Security Checklist

This checklist originally appeared in Department of Energy publication. Not all items in the list will apply to every organization or home user, but it provides a helpful starting point for an organization or individual to review the security of home computer systems. The checklist also includes considerations for organizations that have telecommuting users who regularly access the organization's central network.

User Identification and Authorization
- Is the telecommuter authorized by his or her supervisor/manager to telecommute?
- Is the telecommuter authorized by the system owner to access the system(s) remotely?
- Does the telecommuter have a unique user ID and password for remote access and for access to sensitive applications?

Access Controls
- Are system access controls in place and functioning to log the identification of each remote access user, device, port, and user activity?
- Are system audit logs protected from unauthorized access?
- Are banners displayed regarding monitoring for unauthorized access and misuse?

Auditing
- Does the remote access system record alarms and authentication information?
- Does the system audit log identify date and time of access, user, origin, success or failure of access attempt?
- Are system audit logs retained to support reviews by computer security personnel?
- If dial-up access is allowed, does the system record details of access attempts?

Information Availability
- Are Government information assets (hardware, software, data, records) in a physically secure location and protected from theft, fire, smoke, hazardous material, etc.?
- Is backup media maintained, secured, and easily retrieved to support established contingency and disaster recovery plans?
- Is a physical inventory periodically conducted of Government information assets used for telecommuting?
- Can Government information assets be retrieved in the event of employee termination?
- Information Integrity:
- Is there a process in place to ensure the most current version of antivirus software is installed on the telecommuting computer?
- Are Government information assets adequately secured when not in use by the telecommuter?
- Are user IDs and passwords protected from unauthorized use?

Information Confidentiality
- Is Government information protected from unauthorized disclosure (family, friends, eavesdroppers)?
- Is encryption used when transmitting sensitive unclassified information?

Remote Access Security Administration
- Is organizational, system administrator, and user responsibility for remote access security defined?
- Are justifications for remote access users periodically revalidated to support continued access privileges commensurate with job duties (at least annually)?
- Are incident reporting procedures in place to address handling of security breaches?
- Is regular system monitoring performed to detect unauthorized access attempts, denial of service, or other security weaknesses?
- Is access to network management tools restricted to authorized users?
- Is software used for telecommuting legally purchased, and are software licensing agreements properly maintained?

- Are telecommuting equipment hard drives degaussed or overwritten to remove sensitive information in accordance with established best business practices?

Architecture and Network Topology
- Is the telecommuting equipment used interoperable with the computing architecture deployed at the home office?
- Does the network adequately separate traffic according to user communities?
- Does the remote access equipment and system protect the internal trusted network from the external (public) untrusted network?
- Are network topology maps documented and kept current?

Education, Awareness, and Enforcement
- Are telecommuters and their supervisors trained in the specific risks, threats, vulnerabilities, and proper use of a secure telecommuting environment?
- Is the telecommuter current on his or her computer security training?
- Is the telecommuter aware of the consequences for violation of Condition of Use agreements?

Modem Use
- Is there a single (or otherwise restricted) point of entry via modem into the internal network or server?
- Are all dial-up numbers protected from unauthorized disclosure?
- Is the telecommuter instructed to disconnect modem connectivity to the home office network or server when not in use?

Appendix B. Using Microsoft Personal Security Advisor

Microsoft Personal Security Advisor (MPSA) is a site provided by Microsoft that allows a user to easily check the security and patch state of a Windows NT 4.0 Workstation or Windows 2000 Professional computer (http://www.microsoft.com/technet/mpsa/start.asp). By using this website and associated application, a user can scan their Windows NT/2000 computer and receive a detailed customized report of their computer's security settings and patch level along with recommendations for updates and improvements.

At the time of writing, the following checks are included in MPSA. Microsoft will continue to update this service as additional patches are release or when suggested security settings change.

- Password Strength and Length

- Services

- Macro Virus Protection

- Service Packs

- Hotfixes

- RASMAN

- Auto Login

- Auditing Events

- Secured File System

- Restriction of Anonymous Connections

- Shares

- Unusual Administrators

- Security Zones for Explorer and Outlook

MPSA does have some limitations that users should consider before using:

- The hotfix checking portion of this tool is valid for English-language systems only.

- Presently, MPSA is intended to assess only Windows NT 4.0 Workstation and Windows 2000 Professional.

- MPSA does not check for web server related patches.

- An example scan using MPSA is documented in the following example. To access the MPSA site enter its URL (see above) into the Address Line of the Internet Explorer (note: MPSA requires Internet Explorer 5.0 or later). This will open the MPSA homepage (see Figure B-1).
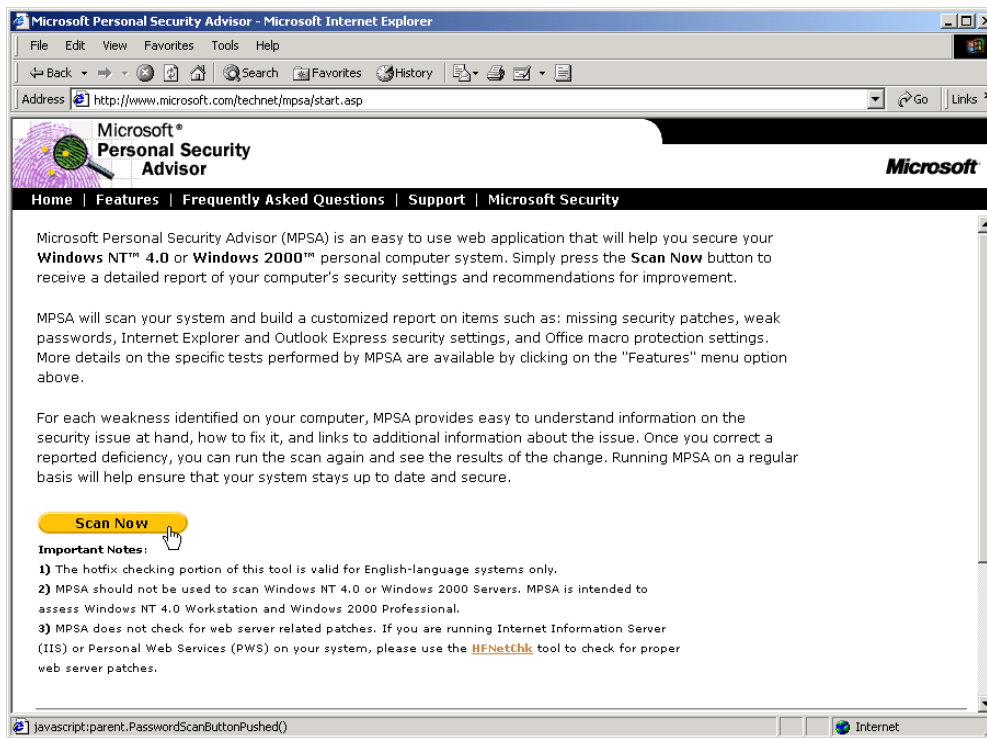
Figure B-1 — MPSA Homepage

To start the scan, press the yellow button labeled "Scan Now". Note: MPSA conducts a scan without sending any sensitive information to Microsoft. MPSA is implemented as an ActiveX control (application). To install and run, you must click the "Yes" button when the Security Warning window pops up (see Figure B-2).

Figure B-2 — MPSA Active-X Control Security Warning

Once a user selects yes, the Active X control is downloaded (this should take less than a minute) and it initiates and processes its scan (see Figures B-3 and B-4).
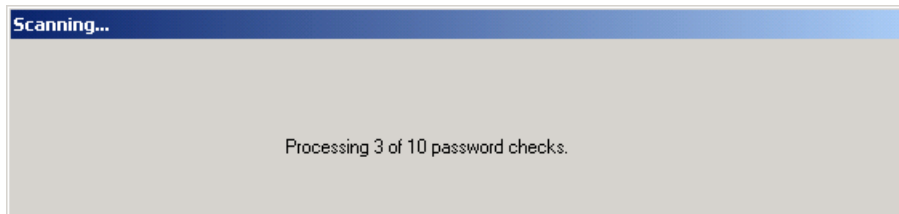
Figure B-3 — MPSA Active Scanning
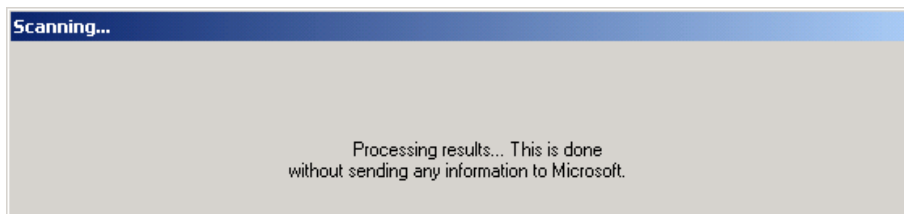
Figure B-4 — MPSA Scan Processing

Once the scan is completed MPSA will generate a report on the overall security and patch level of the scanned computer. Three risk levels are assigned to each item as shown in Figure B-5.

Figure B-5 — MPSA Report Legend

- **Severe Risk**—There is a serious vulnerability in the system, and change is recommended immediately

- **Potential Risk**—There is a potential vulnerability in the system, change is highly recommended.

- **Strong Security**—No vulnerability is detected in the scanned system.

- **Security FYIs**—An issue that may be a vulnerability but requires further investigation.

- **Unable to Scan**—The MPSA was unable to scan for this item.

The final report provides details and advice on each of the tests performed (see Figure B-6).
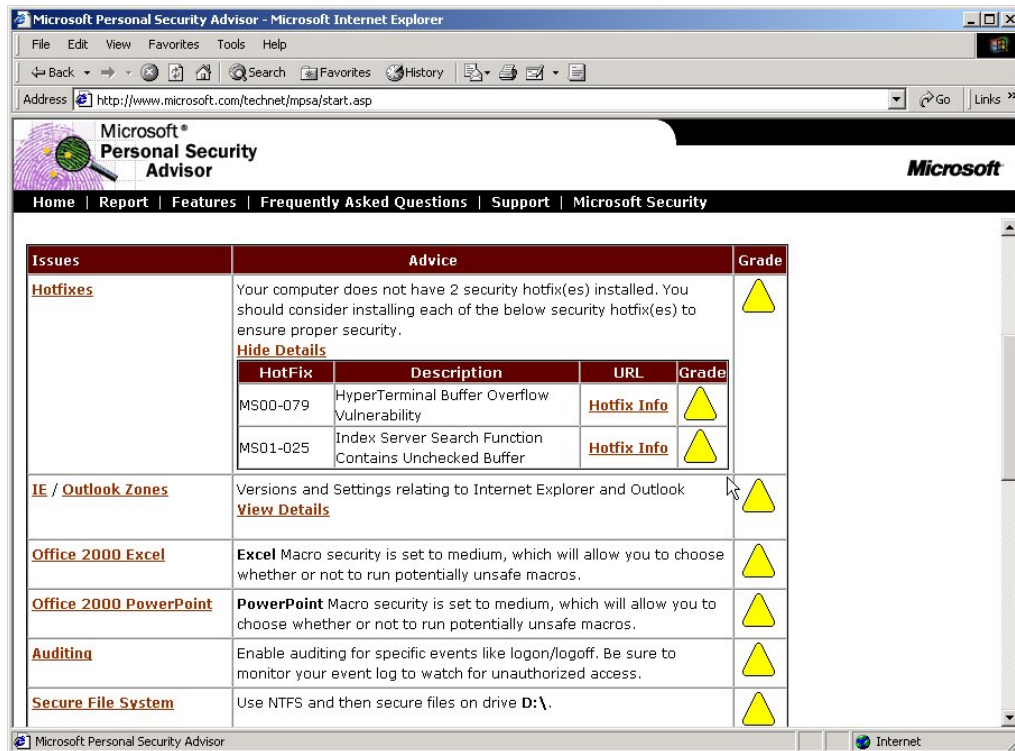
Figure B-6 — Final Report

Clicking on the hyperlinks will provide additional details as shown Figure B-7.
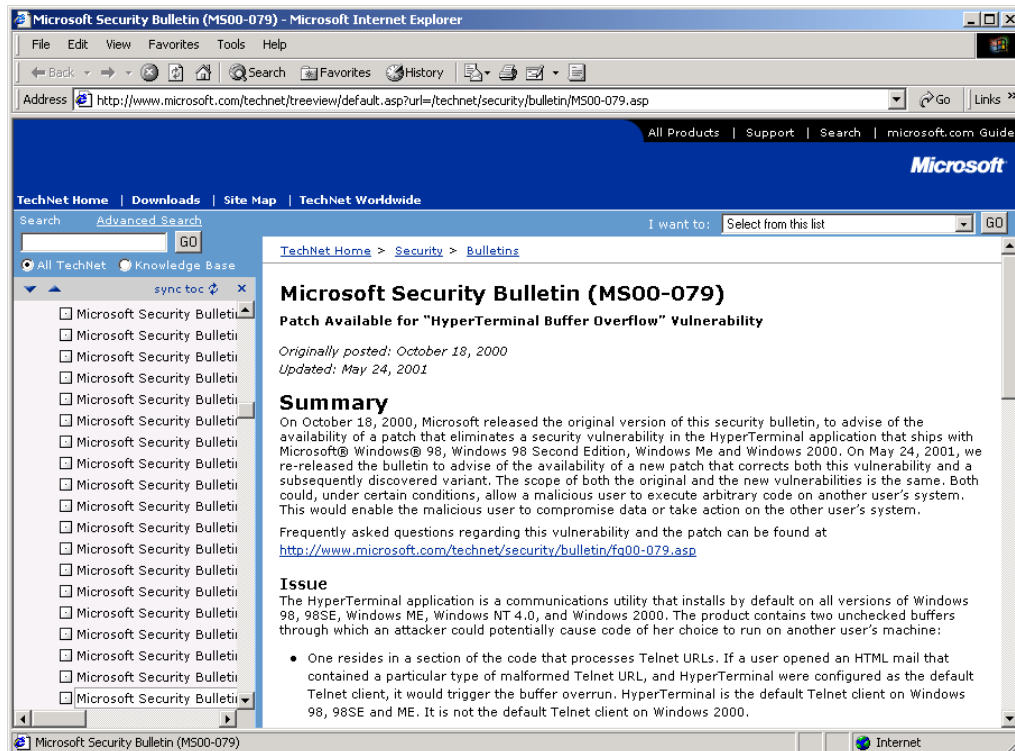
Figure B-7 — Final Report Details

An important point to note when using the MPSA scanner is that it must be run again after any vulnerability is patched. While all steps may be correctly implemented to patch a system, there still exists the possibility that one patch may "unfix" another. For this reason it is important to always scan again to double check for correct operation.

Appendix C. Using Windows Update

Windows Update is a utility provided by Microsoft in most versions of Windows (including some versions of 95 and NT and all versions of 98, ME, 2000 and XP) that allows a user to scan their computer to find any updates that are available at that time from Microsoft and other participating vendors. Figures C-1 and C-2 demonstrate the two different methods of accessing the Windows Update utility. It is suggested that users close all other applications before initiating the Windows Update feature.
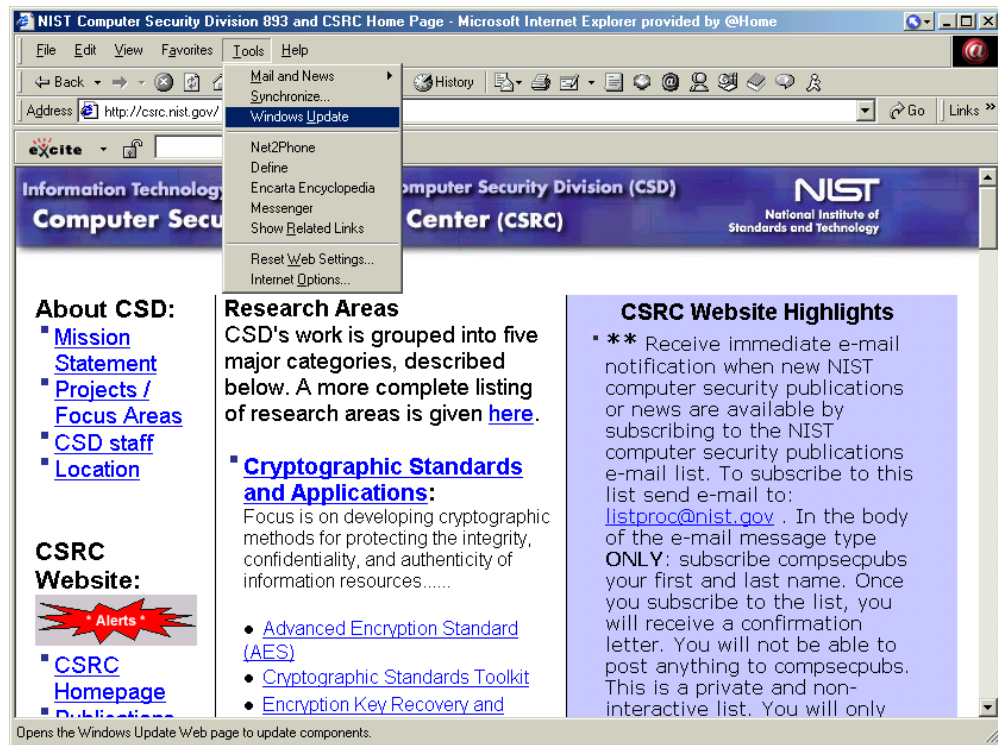
Figure C-1 — Accessing Windows Update Though Internet Explorer

To access Windows update from within Internet Explorer browser, click on *Tools* and then *Windows Update* in the pull-down menu.

Alternatively, a user can access windows update from the Start Menu as demonstrated in Figure C-2. From the Windows desktop, click on the *Start* bar. From the menu, click on the *Windows Update* icon.
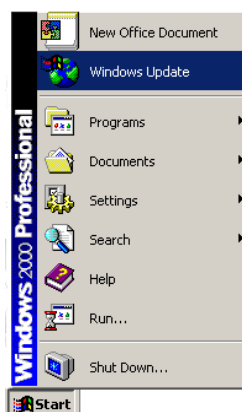
Figure C-2 — Accessing Windows

Either of these options will launch Microsoft Internet Explorer (if it is not already active) and go the Microsoft Windows Update website (htttp://windowsupdate.microsoft.com). See Figure C-3 for the Windows Update homepage.
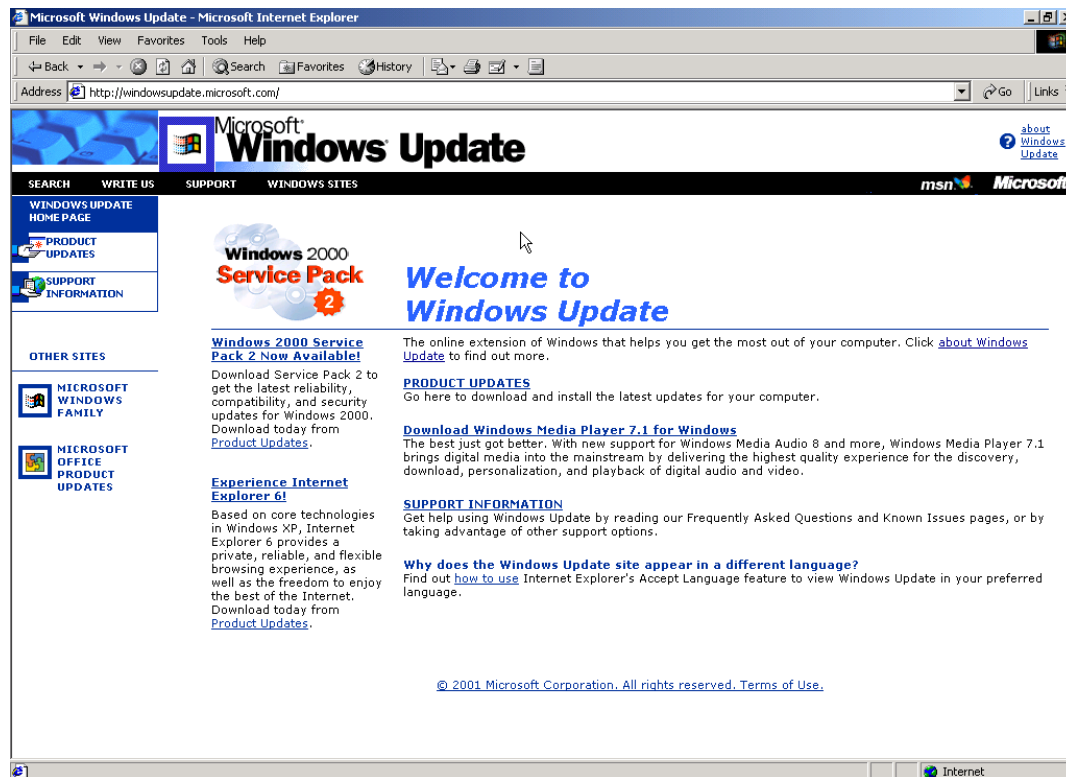
Figure C-3 — Windows Update Homepage

To have the Windows Update scan your computer for updates, click on the "**PRODUCT UPDATES**" link. Note: This is accomplished without sending any information to Microsoft or transmitting sensitive information on your host over the Internet. The Windows Update utility will commence its scan of the user's computer and come up with a customized product update catalog specific to that computer (see Figure C-4). Having Window Update automatically check your system has several advantages. This check assures that users will get the most up-to-date and accurate versions of anything they choose to download from the site. Additionally, they will not waste time downloading components that are already installed.

Figure C-4 — Windows Update Scan

Once Windows Update has finished scanning the users machine, it will generate a list of recommended updates (see Figure C-5). Users can browse the list, decide which components they want, and download them right to their computer.
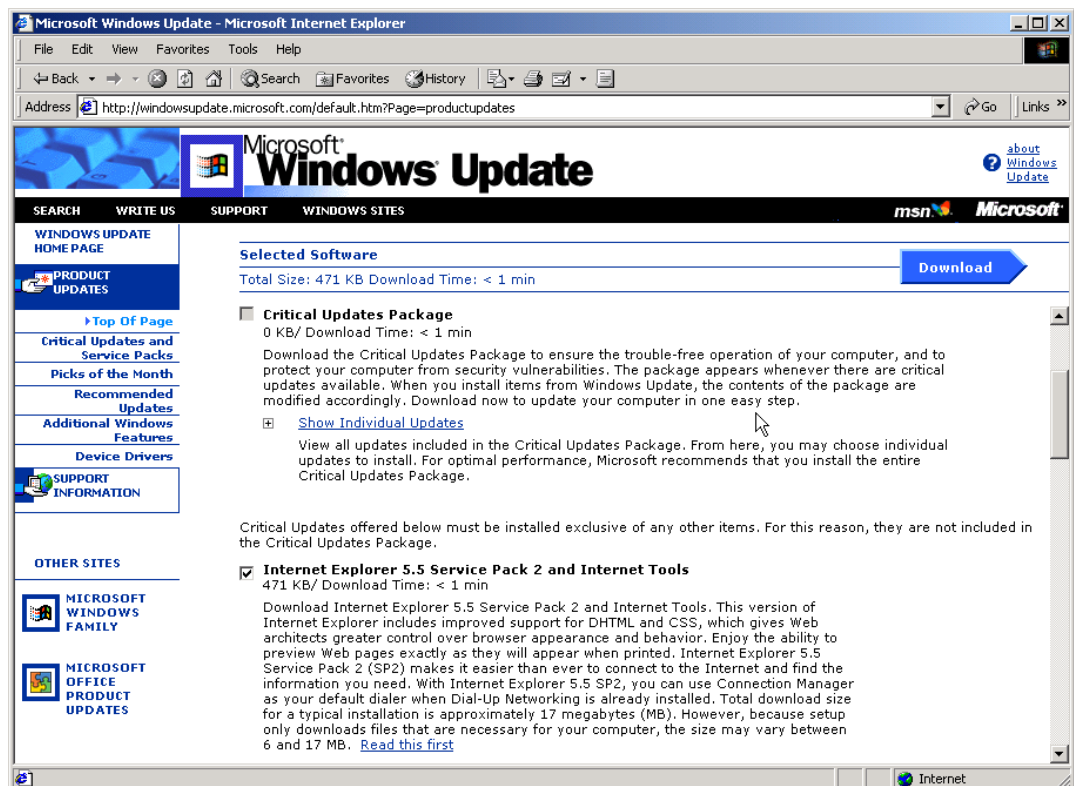
Figure C-5 — Windows Update Recommend Updates

The product updates are broken down into five different sections:

- **Critical Updates and Service Packs**—It is generally suggested that users download all Critical Update Packages as these fix now known problems (often security issues) with their specific installation.

- **Picks of the Month**—These are new releases that add functionality to Windows but are not required to fix a known problem.

- **Recommended Updates**—These are older releases that add functionality to Windows but are not required to fix a known problem.

- **Additional Windows Features**—These are updates to other applications that are included with Windows (e.g., Internet Explorer, Media Player, etc.).

- **Device Drivers**—Listed here will be any updated device drivers for you computer. A device driver is a program that controls a piece of hardware (such as a printer, monitor, disk drive, or video card) that is attached to your computer. Note: Third parties manufacture most hardware and device drivers for this hardware will not be listed here unless the manufacturer has an agreement with Microsoft. Generally a user should go to the appropriate manufacturer's website to get device driver updates.

Certain updates can only be downloaded individually. If this is the case, Window Update will provide notification as shown in Figure C-6. If this happens the user will have to repeat the process delineated here.
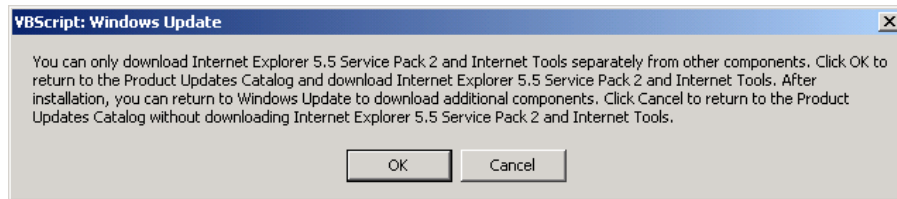
Figure C-6 — Windows Update Multiple Downloads not Permitted Warning

After selecting the patches to download, the Download Checklist page loads to confirm the selections (see Figure C-7). At this point user may choose to view the instructions, start the download and install, or to go back and reselect the software.
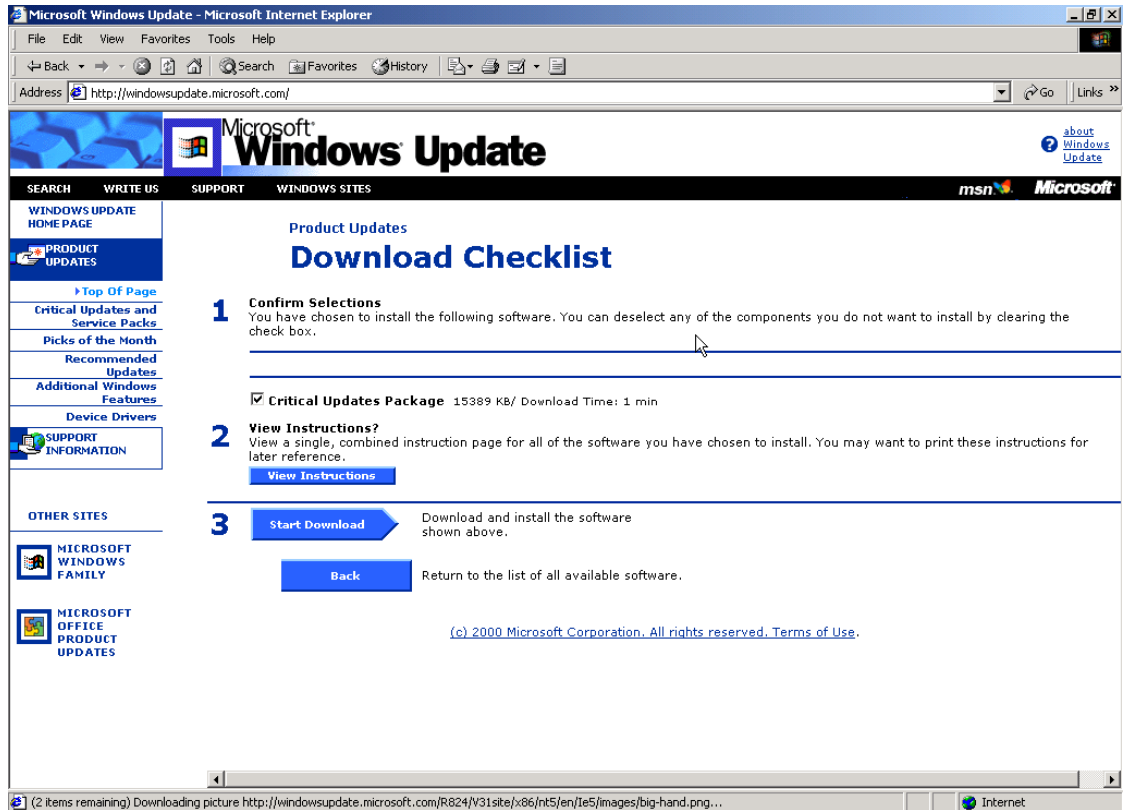
Figure C-7 — Windows Update Download Checklist

After selecting "Start Download" from the Download Checklist page, an additional screen pops up to confirm your selection (see Figure C-8). At this point you may choose to view the instructions, license agreement, start the download and install (by clicking on the "Yes" button), or to go back and reselect the software that you would like to download and install (by clicking on the "No" button).
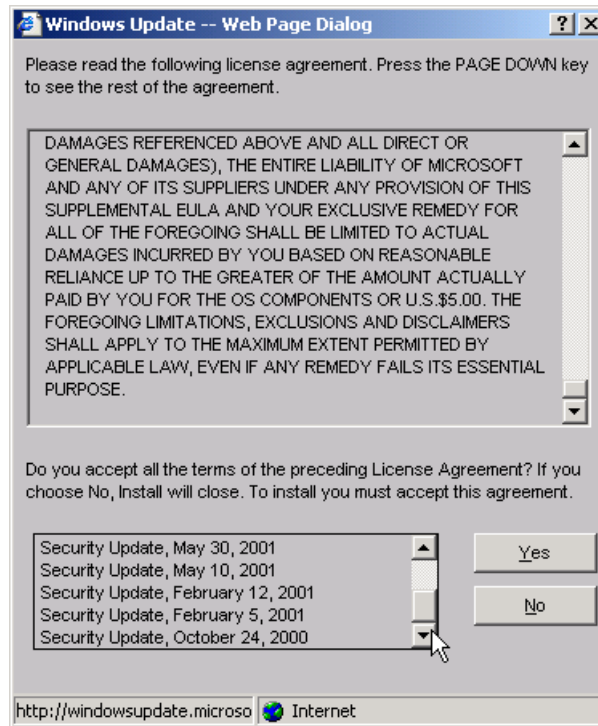
Figure C-8 — Windows Update Confirmation and License Agreement

Upon acceptance of the license agreement, the selected patches and software will be downloaded (see Figure C-9). The duration of the download will depend on several factors including the files size of the software selected and connection speed.
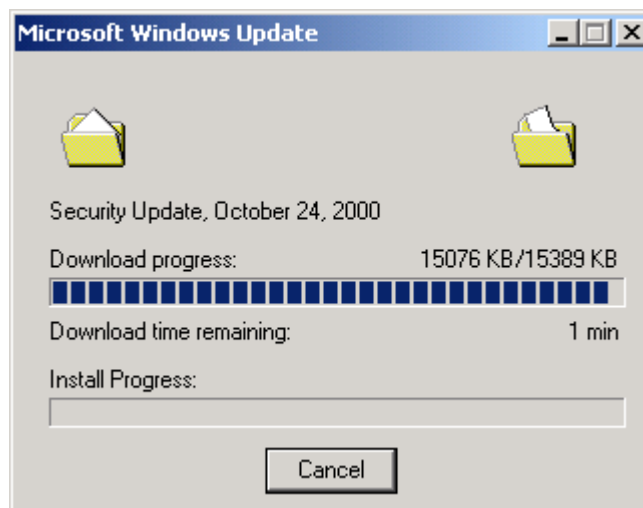
Figure C-9 — Windows Update Download Status Window

After the download is complete, Microsoft Windows Update will start the install process which may take up to several minutes to complete (see Figure C-10).
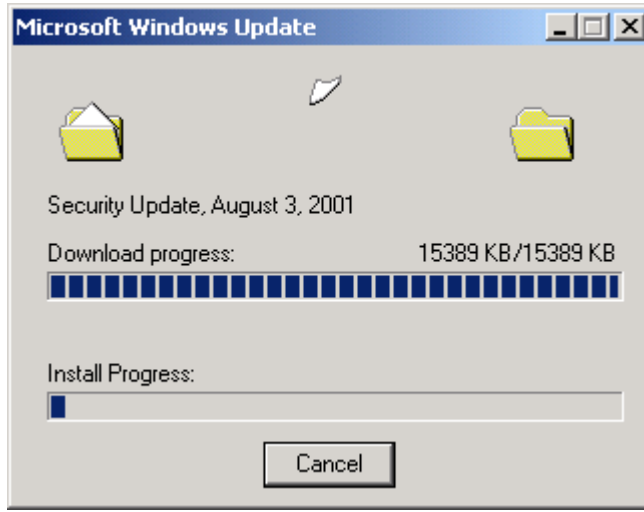
Figure C-10 — Windows Update Install Status Window

Once the install is successfully completed that browser Window will confirm the success (see Figure C-11).

Often, a reboot may be necessary to activate the updates (see Figure C-12). Click on the "Yes" button to restart the computer. Click the "No" button if you do not wish to reboot immediately (changes will NOT take effect until a the computer has successful rebooted). If Window update does not prompt for a reboot, then the changes to not require it and are effective from the time of a successful install (see Figure C-11)
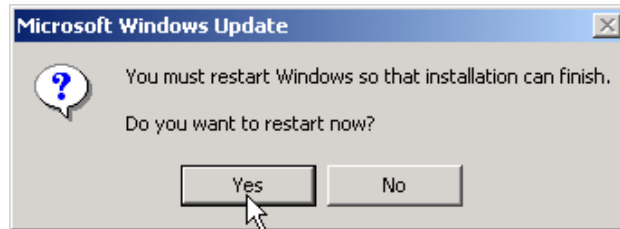
Figure C-12 — Windows Update Restart Dialog Box

If additional patches were required but could not be download simultaneously, repeat the Microsoft Windows Update process as required.

Appendix D. Home Networking Installation Tips

Regardless of the technology chosen for developing your SOHO (small office/home or home office) network, most of the setup steps are similar for each technology with only minor differences in the installation procedures of various types of network media (adapters, hubs and access points, if needed) and between operating systems. Below are some suggestions to assist you in your network setup procedures. The tips are divided into their appropriate category of the network installation/configuration process: planning, network/hardware wiring, PC hardware/software configuration, and troubleshooting.

The tips provided below reference information found on the following websites:

- Computer Emergency Response Center's (CERT) "Home Network Security" http://www.cert.org/tech_tips/home_networks.html

Planning Tips:

The following tips detail planning steps to take before beginning the physical installation procedures of your network. The importance of planning cannot be stressed enough due to the amount of your time it can save.

- Plan out your system installation prior to beginning including: PC physical location, operating systems, network wiring, printers, print drivers, share folders, Internet access, etc.

  If you plan your network design carefully, this can serve to eliminate future problems and bottlenecks. For example, it may not be apparent at the installation time you place two PCs too far apart physically, and used the incorrect cable type to connect them to your switch/hub, but if you plan your steps out in advance you may catch this problem before it occurs.

- Consider keeping a paper record within reach of your design choices such as: local area network (LAN) settings, Internet Service Provider (ISP) network settings, PC descriptions, etc.

  Any user that wants to reinstall the operating system on one of their PCs on their network would benefit greatly from having the necessary configuration information within reach when it came time to specify network settings. Having to stop your work and search for these settings, or contact the appropriate personnel to retrieve them can be very time consuming. Although many users would like to perform tasks all alone, it can be very helpful if you include PC support information such as Technical Support phone numbers in these records as well.

Network Hardware/Wiring Tips:

The following tips describe issues related to network hardware such as switches/hubs and network wiring. Typically network hardware and wiring are more complicated to install/configure, and should be approached carefully.

- If using a network hub or switch with a port labeled "Uplink" connected to an upstream device such as a broadband Internet connection or a secondary hub or switch, be sure not to plug any cables into the port directly adjacent to the uplink port.

This can prevent the uplink port from functioning. The uplink port of a switch/hub and the port directly adjacent to it share internal wiring which when both ports are occupied at the same time can deny all network traffic from reaching your Internet connection or upstream media.

- Take care when determining the physical location of your network hardware such as hub/switch or ISP broadband Internet connection.

  Placing your network equipment near other household equipment such as multi-piece stereos and speakers, large TV/VCR combinations, or even power outlets with more than two outlets can cause interference between the devices which may not be apparent at first but could cause problems in the long run, and even decrease the overall life of the hardware.

PC Hardware/Software Tips:

The following tips describe steps to aide you in the installation/configuration of any PCs attached to your network. These tips describe both hardware and software issues.

- Identify important/critical data on your PC, and conduct a backup of this data prior to modifying your system.

  Although it may not seem necessary, many times there are files that are very important to save in a backup procedure but are not immediately apparent at first. For example, when reinstalling the operating system of a PC, are there any important email messages that you want to save? What about drivers for your graphics board that you downloaded from the Internet and took you an hour to find? Do you use financial software on a regular basis? All of these examples use data files that are vital to normal operating, and should be saved in a backup

- When installing/configuring network adapters, follow manufacturer's detailed instructions.

  As an example, for Microsoft Windows, network adapters that are not recognized by the plug-and-play installation process are sometimes configured manually in a different fashion. The proper installation process is usually detailed within the adapter manual or on the hardware manufacturer's website.

- During installation/configuration of your PCs and components, when prompted, reboot your system as required. (Rebooting will often solve some installation and operational problems).

  The frequency with which you will have to reboot your PC will be determined by which particular operating system and version you run. Hardware and software installation/configuration can make changes to a PC and its operating system that may not take effect until after the PC is restarted. Because of the manner in which operating systems such as Microsoft Windows were constructed, certain types of required settings are only initialized during the boot procedure.

- Keep your original operating system CD-Rom nearby during the installation, as it may be required.

Performing a task such as installing a network adapter, or configuring network settings requires the use of operating system files besides the actual driver for the network adapter. These files may need to be copied from the operating system CD-Rom. An alternate solution is to copy the entire data directory from your operating system CD-Rom onto your hard drive. This will allow you to browse to the local data directory you just created when prompted for a specific file.

- Ensure that the version of any software or file being installed is newer than the one already on your system. If you system already has a newer version that keep that one.

    During the installation/configuration process of your PCs and their components, files are copied from the operating system CD-Rom or data directory that interact with the components you are configuring. In many cases if you have updated your operating system with a service pack or a hot fix, this may replace one of these files, to fix security vulnerabilities, with a newer version. The operating system will prompt you with this alert when it occurs. Be sure to choose to keep the newer file instead of the older one, but read the alert box carefully because the message can be confusing.

- Ensure that your PC is powered off before installing the network adapter to prevent damage to your PC. As an extra precaution you should unplug the AC power cord to the PC.

    Although modern motherboards are designed to protect against minor power mishaps, you should always power down your PC before installing/removing any hardware. This protects you from accidental shocks, and protects your PC's hardware from any mistakes. If cycling the PC's power, always try to wait 10 seconds before turning the power back on again, this increases the life of your hardware.

- Install virus scanning software and update data files frequently for all PCs connected to your network. Run a virus scan once a week.

    Although this may sound repetitive, virus scanners can provide protection against common viruses. Certain virus-scanning software offers a heuristic feature which proactively searches for virus-like activity.

- Develop a regular habit of updating the operating system and major software titles of every PC connected to your network in a timely manner.

    Many major software vendors offer websites that distribute updates and security fixes for their products on a regular basis. Application of these patches is an extremely important step in the installation/configuration process and shows that your work is not complete when the installation finishes. This is especially important for those systems that are connected to the Internet through a broadband connection.

- If you are connecting your network to a broadband Internet connection such as a DSL or Cable modem, it is strongly urged that you implement *both* software and hardware-based personal firewalls.   The hardware firewall provides Network Address Translation to hide the address of your network PCs, while the software firewall can notify you if a Trojan horse program attempts to transmit information without your knowledge.

As described in the section on Personal Firewalls, a broadband Internet connection such as a cable or DSL modem is an "always-on" connection where your PC is connected to the Internet 24 hours a day. This increases the risk for attempts of subversion of your PC. For more information consult the section on Personal Firewalls below.

Troubleshooting Tips:

The following tips detail steps you can take to track down and possibly correct any problems that may arise with your network. They are by no means meant to be a foolproof solution to any type of problem or unpredictable behavior that may arise.

- If using a network hub or switch, consider placing it in an easily accessible location.

  If a problem occurs with your network, and PCs cannot communicate with each other, or cannot reach the Internet, the link lights on the front of your switch/hub can provide valuable information instantly. On virtually all brands of network switches/hubs, sets of link lights give information for each specific port. As an example, if the uplink port on your switch/hub connects your network to your ISP, and this port is not lit, or not lit correctly, then there is a problem with your ISP, and the Internet connectivity in your local neighborhood. In a similar example, if one of your machines is not responding to network requests for resources such as file shares, and the lights for this machine are not lit, or not lit correctly, then there is specific problem with this machine. This quick troubleshooting process can save you valuable recovery time.

- When your PCs aren't responding on the network, and you suspect a network hardware problem, if they are provided on your network adapters, check the link lights on the adapter for a description of the connectivity the adapter has with the switch/hub.

  Similar to the link lights on a switch/hub, the link lights on a network adapter tell more information about the connection or lack of a connection with the rest of the network. Consult the manual for your network adapter to determine what the specific lights mean.

- Have manufacturer technical support information available if necessary

  It is possible to encounter a situation within your network which you cannot solve, or are not informed enough to solve. For this reason, it is important to keep your hardware manufacturer's technical support information available if necessary.

- If available, consider using a cable tester to test network cables for faulty wiring. Network testers can be purchased at any major PC retailer, and a variety of specialty shops.

  Even if you are not crimping your own network cables, they are still subject to failure by getting ripped or torn in your household or small office. A user could accidentally kick or rip a cable that was run across a floor, instead of inside of a wall, and cause the internal wires to break or tear. Even if the tear is not evident externally, a single wire that is torn inside a length of network cable can cause the entire length not to function correctly.

Please note that it is important to exercise extreme caution if you follow any of the tips provided due to the fact that not all of the tips described above may apply to every networking setup.

Appendix E. Online Resources

A wealth of security information is available on-line. The following list of Web sites contains a number of notable sites where one can begin to explore additional information on computer security.

Federal Government Resources

Telework.gov - http://www.telework.gov/

Telework.gov is an interagency site maintained by the General Services Administration (GSA) and the Office of Personnel Management (OPM). It provides a central clearinghouse for information on telework and telecommuting practices and policies from both civilian and military agencies.

ICAT Metabase - http://icat.nist.gov

ICAT is a searchable index of information on computer vulnerabilities. It provides search capability at a fine granularity and links users to vulnerability and patch information.

Computer Security Resource Clearinghouse (CSRC) - http://csrc.nist.gov

The CRSC contains current US security policy documents, calendar of events, security publications, training resources, and information on various computer security subjects.

The Federal Computer Incident Response Capability (FedCIRC)
   http://www.fedcirc.gov/

FedCIRC provides a government focal point for incident reporting, handling, prevention and recognition.

National Information Assurance Partnership (NIAP) - http://www.niap.nist.gov/

NIAP is a U.S. Government initiative to promote the development of technically sound security requirements for IT products and systems and appropriate metrics for evaluating those products and systems to meet the needs of both information technology (IT) producers and consumers.

Universities and Professional Societies

Computer Emergency Response Team (CERT) Coordination Center –
   http://www.cert.org

CERT issues security advisories, helps start other incident response teams, coordinates the efforts of teams when responding to large-scale incidents, provides

training to incident response professionals, and researches the causes of security vulnerabilities. http://www.cert.org/

WWW Consortium Security FAQ - http://www.w3.org/Security/FAQ

The World Wide Web Consortium site contains a repository of information about the World Wide Web for developers and users.

RISKS forum - http://catless.ncl.ac.uk/Risks

ACM Committee on Computers and Public Policy forum on risks to the public in computers and related systems. http://catless.ncl.ac.uk/Risks/

Center for Education and Research in Information Assurance and Security (CERIAS) http://www.cerias.purdue.edu/

CERIAS is a university center for multidisciplinary research and education in areas of information security (computer security, network security, and communications security), and information assurance.

Commercial Resources

Microsoft Internet Explorer Security Page http://www.microsoft.com/windows/ie/security/default.asp

Microsoft posts information and code fixes for security problems here as soon as they are available.

Netscape Security Page - http://home.netscape.com/security/notes/

Latest news concerning the security of Netscape's client, server, and development software can be found here

System Administration, Networking, and Security (SANS) Institute – http://www.sans.org

The SANS community creates four types of products and services: system and security alerts and news updates, special research projects and publications, in-depth education, and certification. http://www.sans.org

References and Further Reading

CableModem.net. "Broadband Internet Security Basics - The ABCs ... and XYZs of protecting your always-on, high-speed connection",
http://www.cablemodem.net/features/mar00/story1.html

CERT. Home Network Security 22 June, 2001.
http://www.cert.org/tech_tips/home_networks.html

DSL Reports. "DSL FAQ", May 2000.
http://www.dslreports.com/faq

Firewall Guide.com. Firewall Guide Software Reviews.
http://www.firewallguide.com/software.htm

Frankel, Sheila. *Demystifying the IPsec Puzzle*, Artech House Publishers, 2001.

National Institute of Standards and Technology. "Guide to Firewall Selection and Policy Recommendations", DRAFT. November, 2001.
http://csrc.nist.gov/publications/drafts/Firewall-Guide.pdf

National Institute of Standards and Technology. "Guidelines on Active Content and Mobile Code", SP 800-28. October 2001.
http://csrc.nist.gov/publications/nistpubs/800-28/sp800-28.pdf

National Institute of Standards and Technology. "Security Self-Assessment Guide for Information Technology Systems", SP 800-26. August, 2001.
http://csrc.nist.gov/publications/nistpubs/800-26/sp800-26.pdf

National Institute of Standards and Technology. "Generally Accepted Principles and Practices for Securing Information Technology Systems", SP 800-14. September 1996.
http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf

Hillman, Dale. "How Complicated Is Home Protection?", November 23, 2000.
http://www.sans.org/infosecFAQ/homeoffice/protection.htm

Zych, Tina. "Personal Firewalls: What are They, How Do They Work?", August 22, 2000.
http://www.sans.org/infosecFAQ/homeoffice/personal_fw.htm

Index