



# Protecting Computers at Home

**Paul Krystosek**

**William Orvis**

**DOE CIAC**

**US DOE 2002 Computer Security Group**

**Training Conference**

**Phoenix**

**May 1, 2002**

# LLNL Disclaimer

---

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

*Reference to any specific commercial product does not necessarily constitute or imply its endorsement, recommendation or favoring by CIAC, the University of California, the United States Department of Energy, or the United States Government.*

# Your Home Computer Might Be More Than You Think It Is

---

- A conduit to the inside of your company firewall.
- An attack site for compromising other systems.
- A spy on you and your family.
- A denial of service drone.
- A worm breeding ground.



# Are You A Pipe to the Inside? . . . . .

- You have a VPN or other encrypted link open to the inside of your company firewall.
- An intruder compromises your machine and uses the link to get inside the company firewall.

**This has happened. A system with a modem connection to an ISP and an ISDN connection to the inside of a company firewall was compromised through the modem. The intruder then went through the ISDN connection to the company.**

# Are You Attacking Others? .....

- A system is compromised and used as a platform to attack other systems.



**This has happened. During the BIND/named attacks in 1998, hundreds of home computers were compromised and used to expand the attack.**

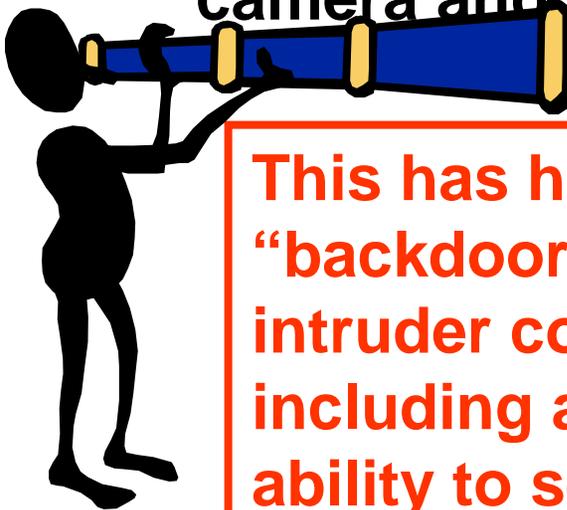
U.S. Department of Energy

**CIAC**

Computer Incident Advisory Capability

# Is Someone Watching You? .....

- An intruder with access to your home machine can read all your documents and capture your connections to other systems (banks, workplace, etc.).
- An intruder with access to your home machine can turn on the microphone and camera and see inside your home.



**This has happened. Remote control “backdoors” (Back Orifice) give a remote intruder complete control of your system, including a view of your desktop and the ability to see and move your mouse.**

U.S. Department of Energy

**CIAC**

Computer Incident Advisory Capability

# Are You a DoS Drone?

---

- A compromised machine can have denial of service drone software installed.
- Drone workstations work under the control of a master who directs them to start a denial of service attack on selected targets.

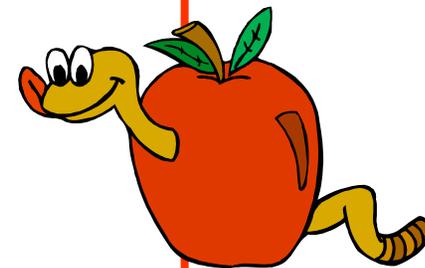
**This has happened. The DoS attacks of 2000 were performed by multiple home machines used as Drones to attack Internet commerce sites.**

# Are You a Worm Breeder? .....

- A worm program is delivered by a web page, e-mail attachment, or ICQ message.
- The worm is activated by clicking on it and starts sending worm infected mail or attack packets all over the Internet.

**This has happened. I Love You, Melissa, Nimda, MTX, FunLove, Hybris, Gibe, Glacier, Ramen, Code Red, Anna Kournikova, Sircam, Nimda ...**

**Need I go on?**



U.S. Department of Energy

**CIAC**

Computer Incident Advisory Capability

# How Can This Happen?

---

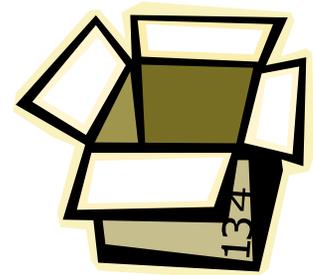
- **Most operating systems are not secure out-of-the-box.**
- **Internet usage habits increase the risk of intrusion.**
- **New Internet connection capabilities also increase the risk.**



# Most Operating Systems are Not Secure Out-of-the-Box

---

- Vulnerabilities have been found after the software went to manufacturing.
- Installers install everything possible on a system to make it appear “Feature Rich” (Marketing).
- Default accounts, passwords, and unprotected services make a system easier to install but are known by the intruder community.



**We have seen new systems compromised within minutes of being plugged into the net.**

# Internet Usage Habits Increase the Risk of Compromise

---

- People are spending more time online through a dial-up modem connection which increases the window for an attack.
- People are visiting any website that interests them including some run by intruders.
- Some people are willing to double click on anything.



**We have seen systems compromised through the modem connection while the user was browsing.**

# New Internet Connection Capabilities Also Increase the Risk

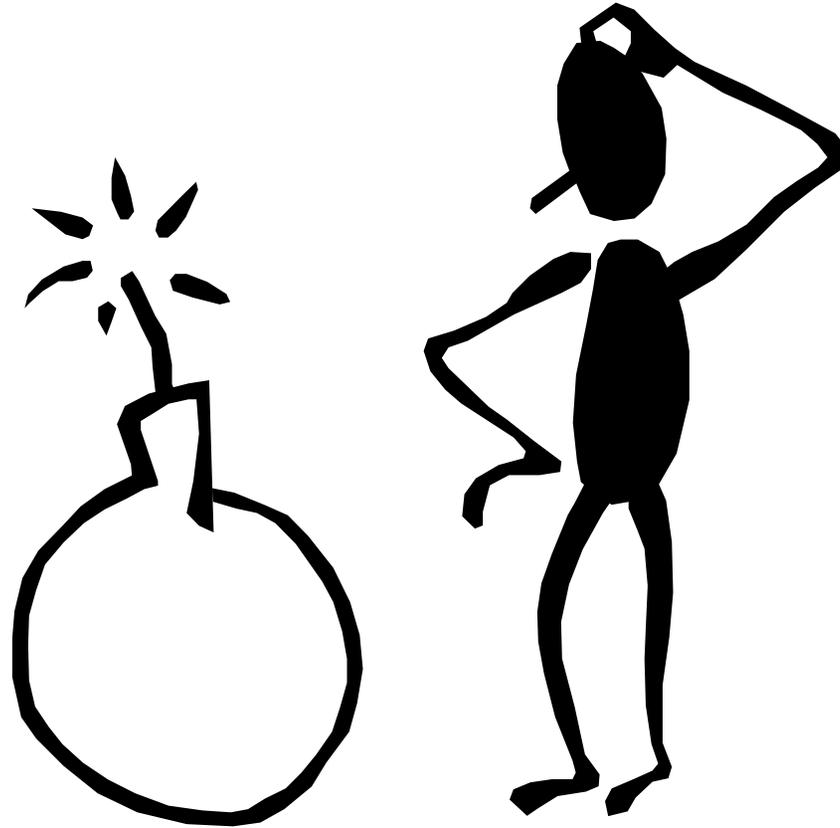
---

- Broadband connections (cable modems, DSL, ISDN) are on all the time which increases the window for attack.
- Broadband systems are also sought by intruders because of their speed and reliability.

**We have seen hundreds of home computers on a broadband network that were compromised and used in an attack.**

# What Can You Do???

---



# Create An Electronic Security Perimeter Around Your Home System...

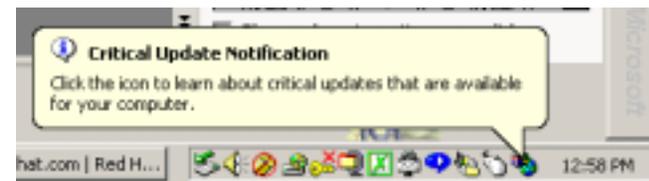


- **Keep your computer systems up-to-date.**
- **Eliminate unneeded services.**
- **Do not use services that pass the password in the clear.**
- **Use good passwords and understand what they protect.**
- **Use an antivirus program with realtime virus detection.**
- **Create a security barrier between you and the Internet (encryption, firewall, NAT, etc).**

# How Do You Keep a Windows System Up-To-Date?

---

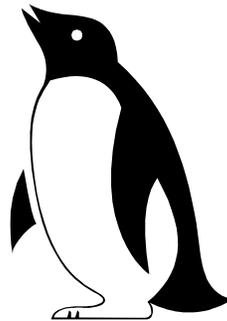
- Visit Windows Update often and install any critical updates.
  - <http://windowsupdate.microsoft.com>
  - Windows 95 users will need to download and install most updates by hand as it is no longer supported.
- Check security bulletins for problems.
  - CIAC <http://www.ciac.org>
  - Microsoft security bulletins.
    - <http://www.microsoft.com/technet/security/current.asp>
- Install Critical Update Notification (included in new versions of windows) to let you know when new critical updates are available.
  - <http://windowsupdate.microsoft.com>



# How Do You Keep A Linux System Up-To-Date?

---

- **Watch security bulletins for potential problems.**
  - CIAC <http://www.ciac.org>
  - RedHat <http://www.redhat.com/solutions/security/>
- **Watch vendor security alerts for all your installed products.**
- **Download and install updated packages when called for in a security bulletin. Don't install package updates for services you are not using.**



# How Do You Keep a Macintosh Up-To-Date?

- **Install Software Update to automatically update your system or watch the security updates page.**
  - [http://www.apple.com/support/security/security\\_updates.html](http://www.apple.com/support/security/security_updates.html)
- **Watch security bulletins for potential problems.**
  - CIAC <http://www.ciac.org>
- **Watch for vendor security alerts for all your installed software.**
  - Apple Security-Announce mailing list <http://lists.apple.com>



# Why Should You Eliminate Unneeded Services?

---

- **A service is software that provides information through a networked port.**
- **Every open network port is another way into a system that could be compromised.**
- **If a port is closed, it cannot be compromised.**
- **If the service software is not on a system, it cannot accidentally be started up.**
- **It is not difficult to reinstall a service if you need it at a later time.**

# How Do You Remove Services From Windows?

---

- **Uninstall with the Add/Remove Programs control panel.**
- **Turn off in a control panel if they cannot be uninstalled.**
- **Use IPSec to block access to all but specific ports.**



# How Do You Remove Services From Macintosh OS 9?

---

- **Disable with the Extensions Manager control panel.**
- **Remove the extension that controls the service from the System Folder directory (/System Folder, /System Folder/Control Panels, /System Folder/Extensions, /System Folder/Startup Items).**

# How Do You Remove Services From Macintosh OS X?

---

- **Turn off in Sharing control panel**
  - FTP, Web, SSH
- **Comment out in /etc/inetd.conf Some control panels do this for you.**
- **Move files out of /System/Library/StartupItems**
  - The system tries to start every item in this directory.
  - The startup of some items is controlled by /etc/hostconfig

# How Do You Remove Services From LINUX

---

- **Comment out the service in inetd.conf.**
- **Remove the startup file from rc2.d or use the Runlevel Editor control panel.**
- **Use Serviceconf with RedHat to turn services on and off.**
- **Remove the service executable files from the system.**
  - Remove with package manager (rpm)
  - Remove by hand (you must know where the files are).

# Don't Use Services That Leave the Login Unprotected

---

- **Older communications services pass a password in the clear over the network that any listening machine can capture.**
  - FTP, Telnet, rsh, rlogin
- **Use instead services that use encryption or a challenge-response (one-time password) method of authenticating.**
  - SSH, VPN, Opie (s-key), LanManager2, NTLM, AppleShare

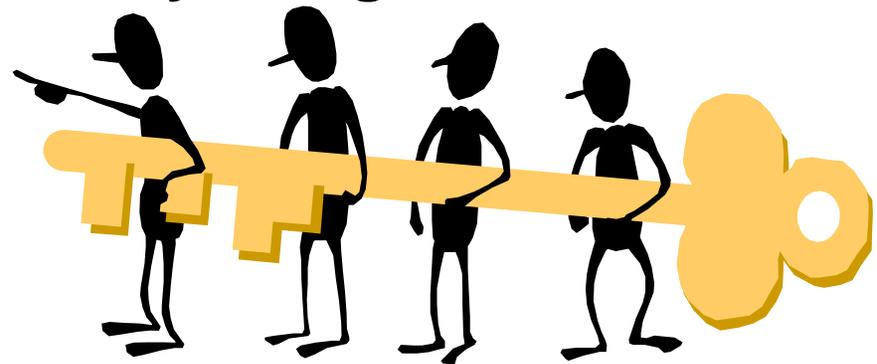
# Do You Know What Your Password Does?

---

- On Windows 95, 98, and ME the login password unlocks the password file which contains passwords for networked resources. It does not control access to any files on the local machine.
- On Windows NT, 2K, XP, Macintosh OS X, and LINUX, the login password controls access to the local files.
- On Macintosh OS 9 – What password?
- In all cases, passwords are required for network logins.

# What's a Good Password

- It used to be that a password just had to be hard for a person to guess.
- Now it must be hard for a program to guess.
- Maximize the “key space” by using different kinds of characters.
  - lower case
  - upper case
  - numbers
  - symbols
- To stop dictionary attacks, do not use a word out of a dictionary, any dictionary.



# Be Careful When Saving Passwords for Networked Resources

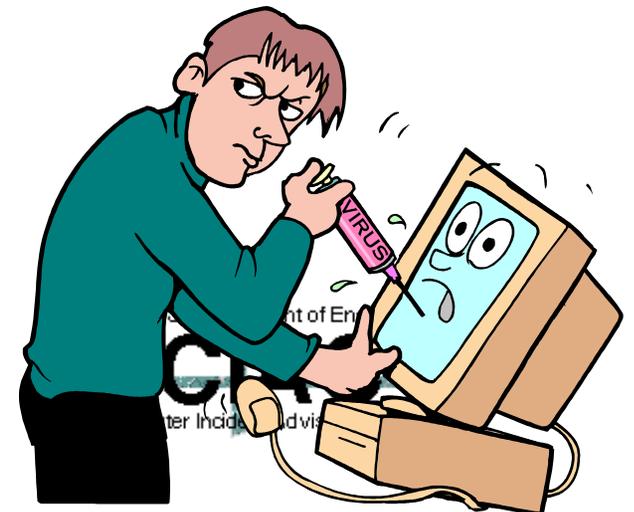
---

- Anyone who can unlock your password file has access to all of your networked resources.
- Anyone who compromises your system while you are logged on has access to all your network resources.
- Use encryption or challenge response when logging into a networked resource to prevent it from being sniffed.
  - Yes: SSL, HTTPS, SSH, Smart Card, Windows Login
  - No: FTP, telnet, rlogin, rsh

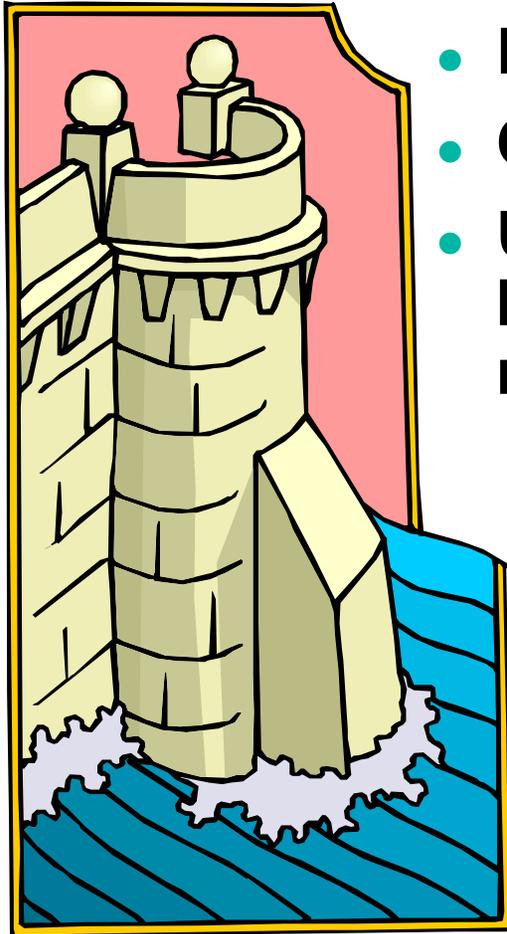


# Use Current Antivirus Software .....

- Use current software.
- Get regular software and signature updates from your vendor.
- Subscribe to automated updates (~\$10/yr).
- Turn on the realtime scanner to detect infected files when they are accessed or downloaded. Scan both incoming and outgoing mail.



# Create a Security Barrier



- Protect simple dial-up connections.
- Create a secure home network.
- Use protected connections (encrypted) between you and the company network.

# How Do You Protect a Simple Dial-up Connection?

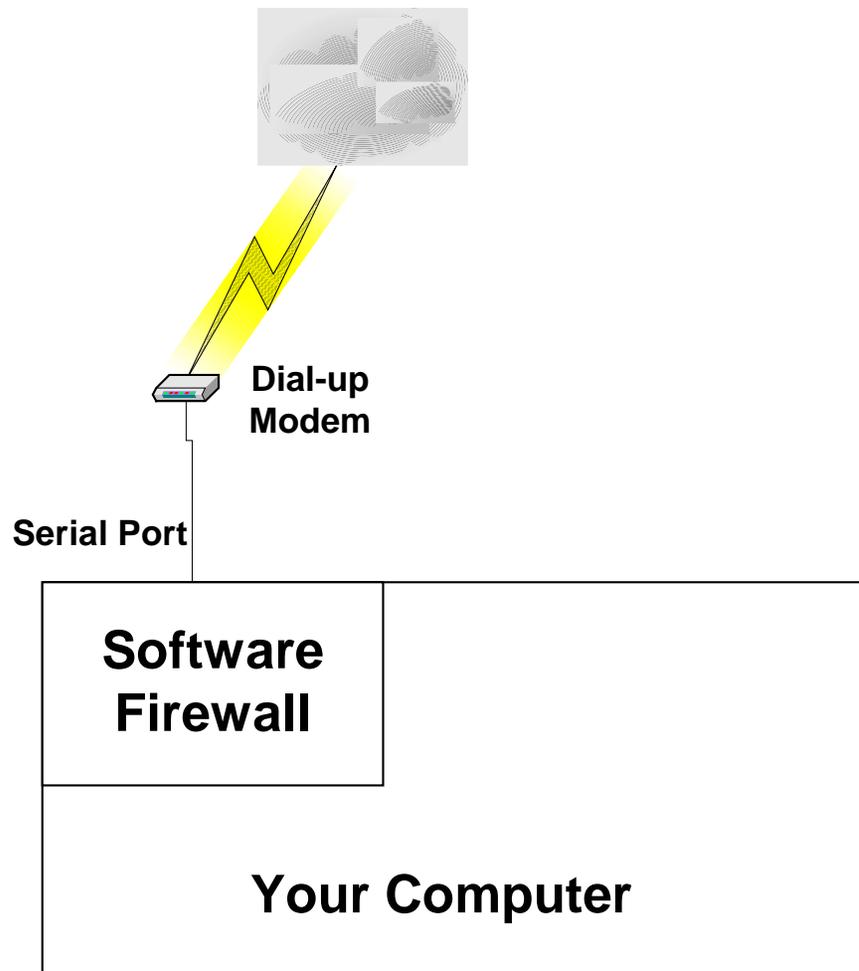
---

- **Software Firewall**
  - Provides incoming protection
- **File authorization program**
  - Provides outgoing protection
- **Built-in firewalls**
  - Windows 98 and later
  - Mac OS-X
  - Linux



# Protect One Computer with Dial-up Connection

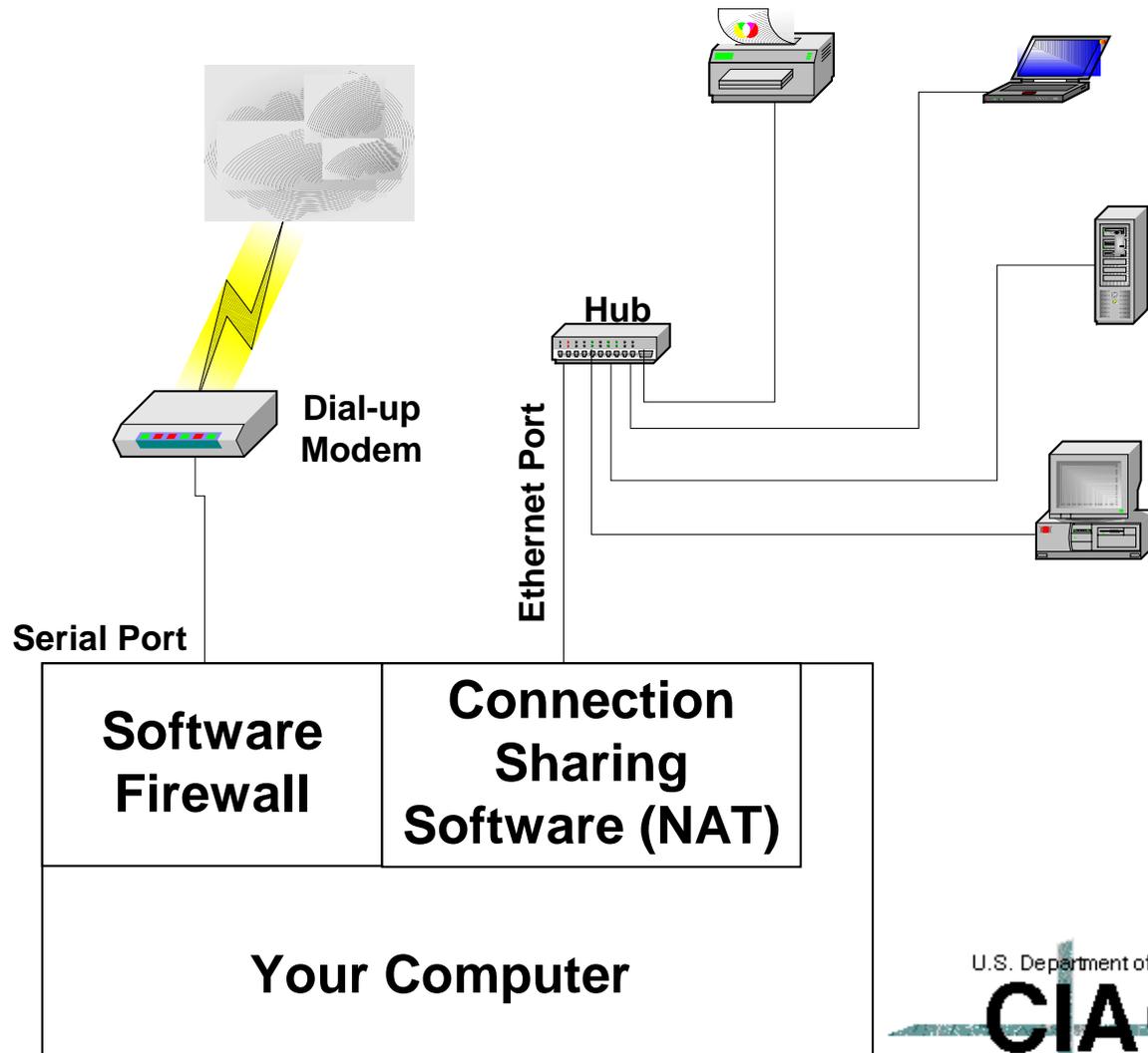
---



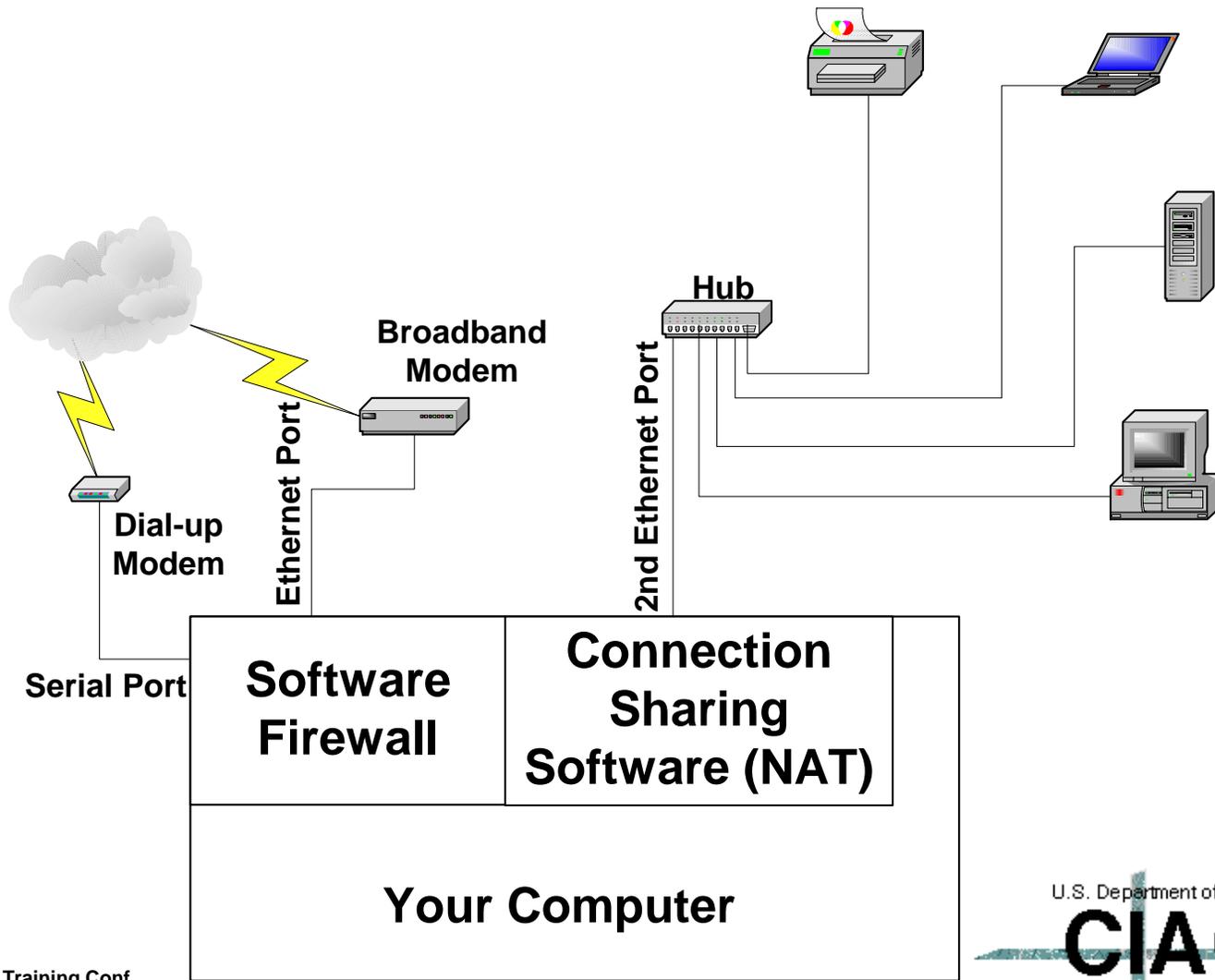
# **Home Networks Have More Options . . . .**

- **Software based protection**
  - **Software firewall**
  - **Software connection sharing with NAT**
- **Hardware based protection**
  - **Hardware firewall with packet filtering and NAT**
  - **Hardware firewall with stateful packet inspection and NAT**

# Protect Home Network with Dial-up Connection



# Setting Up a Home System With a Software Firewall



# How Do You Create a Security Barrier?

---

- Install a Firewall between your home network and the Internet.
- Use Network Address Translation (NAT) to hide the addresses of internal machines.
- Most Firewalls do NAT.

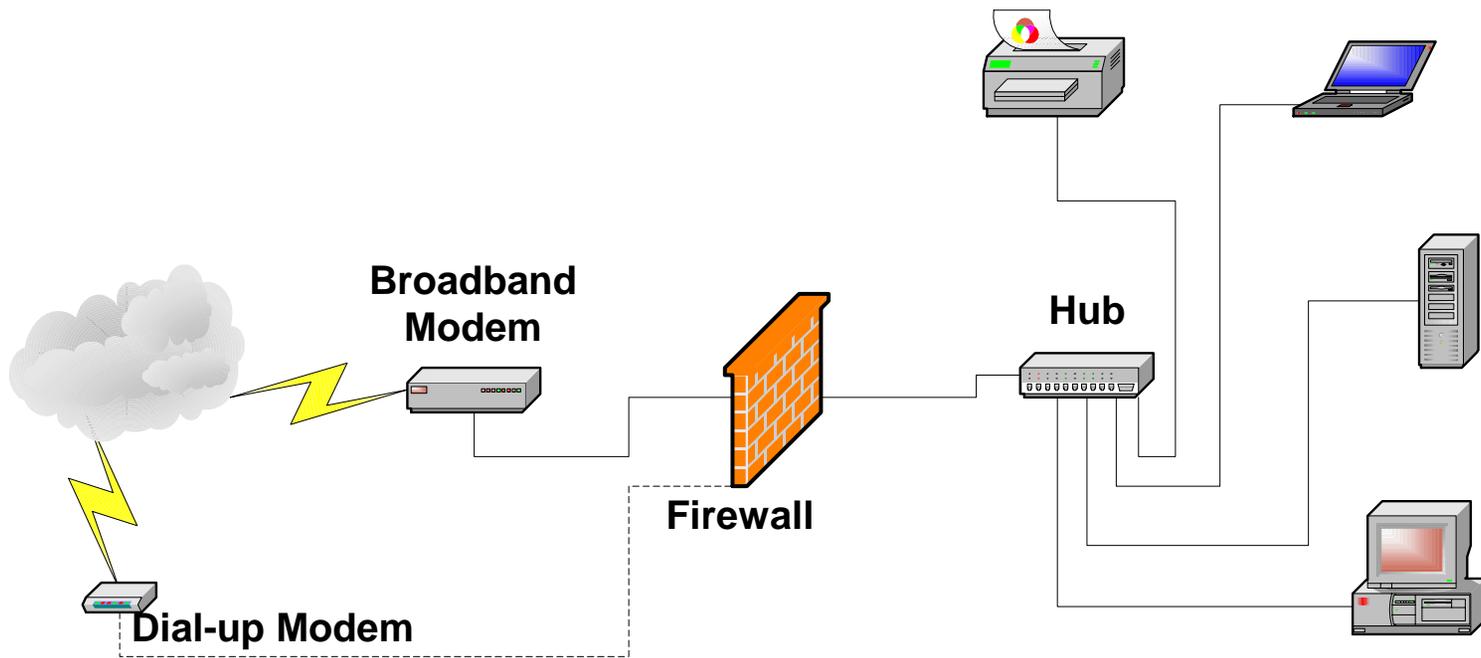
**A side benefit of NAT is that you can share one external IP address among multiple internal machines, saving you money. You save enough to pay for the firewall in less than 2 years.**

# Firewalls Control Access To A Network

---

- **A firewall controls what kinds of communications can go into or out of a network.**
- **The simplest firewall blocks all incoming connections and allows all outgoing connections.**
  - **The direction of a connection is determined by who started it. Inside to outside = Outgoing.**
  - **It may allow an incoming connection to a specific service on a specific internal machine.**
  - **It uses NAT to hide the internal machines.**

# Setting Up a System With a Hardware Firewall

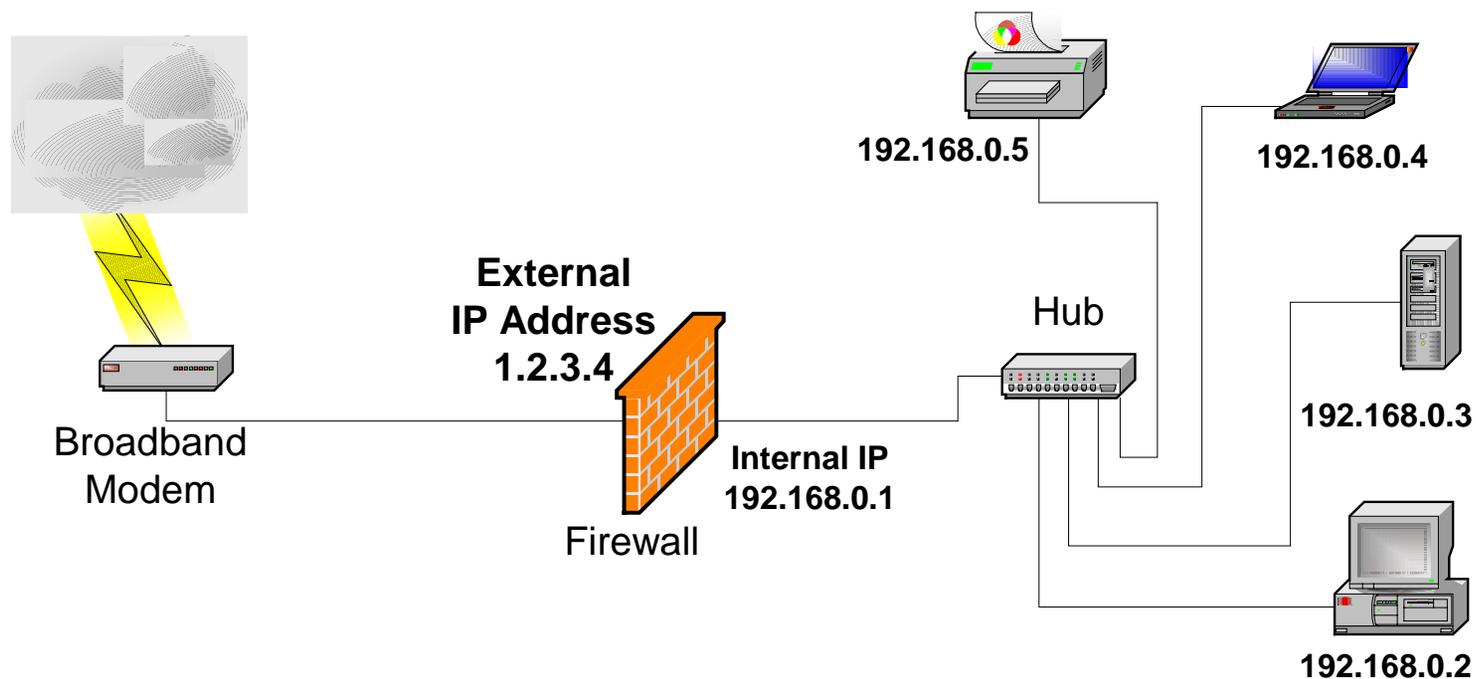


# Internal Systems are Hidden With NAT

---

- NAT uses unroutable addresses for machines inside the firewall and legal addresses outside of the firewall.
- When information passes through the firewall, the packet addresses are translated between the unroutable internal and routable external addresses.
- If there is a leak or cross connection between the inside and the outside, communications stop at the first router, protecting the internal machines.
- Multiple internal addresses can share one or a few external addresses.

# How Does NAT Help Protect a Home Network?



# What Are the Tradeoffs Between the Different Types?

## Software

- **Less expensive (~\$50). Built-in to Win XP.**
- **Do not do NAT. Windows 98 and later do connection sharing (NAT).**
- **Could be compromised along with the multi-mission system they are protecting.**
- **Outgoing file authorization protects against becoming a virus spreader or DoS drone.**
- **Can detect specific types of attack but must be updated regularly.**

## Hardware

- **Slightly more expensive (~\$150).**
- **Do NAT internally.**
- **Single Mission Systems.**
- **They are extremely difficult to compromise.**
- **If they are compromised, they cannot do anything.**
- **They cannot do outgoing file authorization.**
- **Most do not detect specific types of incoming attacks.**

# More Tradeoffs Between the Different Types

## Software

- Work with modem or Ethernet connections to the Internet.
- Most protected machines cannot be used as servers.
- Connection sharing can slow your workstation.
- Your workstation must stop what it is doing and deal with every incoming packet.

## Hardware

- Work with Ethernet connections to the net. Only a few can drive a modem.
- One server allowed (per service).
- Connection sharing is handled by the firewall.
- Internal networks are much quieter as all unwanted, incoming packets are blocked.
- Some have problems with peer to peer connections (networked games).
- Options include, built-in hub, print server, wireless hub, VPN.

# Which Firewall to Use? .....

---



# What's Available?

---

These are only a few of the software and hardware firewall manufacturers.

## Software Firewall

- Iss (NetworkICE)
- McAfee
- SyGate
- Symantec (Norton)
- Tiny
- ZoneLabs (ZoneAlarm)

## Hardware Firewall

- Asante
- D-Link
- Hawking
- Linksys
- MultiTech
- NetGear

Note that many of the software products are free for personal use. This list is not comprehensive. Check <http://www.firewallguide.com> and <http://www.homenethelp.com> for information and a list of more products.

# You Have a Single Machine With a Dial-up Connection

---

- **Use a software firewall.**
- **Use a file authorization firewall to protect against being a drone or worm breeder.**
- **Do not leave the connection open when you are not using it.**
- **Most hardware firewalls cannot use a modem and provide many features that you will not use.**

# You Have a Single Machine With a Broadband Connection . . . . .

---

- **Use a software firewall or one of the simpler hardware firewalls.**
- **Use a file authorization firewall to protect against being a drone or worm breeder.**
- **Turn your system off when it is not in use.**
  - Saves power.
  - Reduces wear on your system.
  - Reduces the window of opportunity for attack.
- **Use a hardware firewall for increased protection.**

# You Have a Home Network With A Dial-up Connection

---

- You need a fast workstation with a software firewall and connection sharing, or a hardware firewall that can dial a modem.
- Be sure your hardware firewall + modem works with your ISP.
- Use a software file authorization firewall on each internal machine to protect against being a drone or worm breeder.

# You Have a Home Network With a Broadband Connection

---

- **Use a hardware firewall.**
  - It offloads the networking from your workstation to the firewall.
  - It quiets the internal network.
  - It lets you share a single connection among multiple machines.
  - It is much faster and does not load your main system.
- **Use a file authorization firewall on each internal machine to protect against being a drone or worm breeder.**
- **Consider a hardware modem with built-in wireless switch if you move around a lot or don't have wires where you need them. (Hardwires are faster and more secure.)**

# If You Are a 'Techie' At Heart .....

- Consider a 'home made' hardware firewall.
- Use an old PC that is gathering dust in the garage.
- Install a Linux firewall.
- A Linux firewall gives you more control over incoming and outgoing packets.
  - Install a minimal Linux system.
  - Use the ipchains command to control packet forwarding between two Ethernet cards.
  - See: <http://www.redhat.com/support/resources/networking/firewall.html>
  - See also ipfilter/iptables project <http://www.netfilter.org/>

# Use Protected Connections to Your Company Network

---

- **Encrypted connections protect company data and login information.**
- **VPN – Makes you appear to be on the internal company network.**
- **SSH – For point to point connections (terminal logins) or file transfers with internal machines.**
- **Websites with sensitive data should require an SSL connection (https).**

# Networking Extends Beyond the Wires

---

- Home network security is not a “DOE only” activity, don’t forget to help your family and friends do the same.
- Show people how easy it is to install and configure a home firewall and they will tighten up their own systems.
- The fewer vulnerable systems out there, the less likely you will be attacked.

# What Are You Going to Do When You Get Home?

---

- Make sure your home systems are up-to-date.
- Eliminate all unneeded services from your systems.
- Eliminate services that send passwords in the clear.
- Change your passwords to new, strong ones.
- Make sure your antivirus software is current.
- Create a secure home net.
- Help your neighbors.
- Be careful out there!



U.S. Department of Energy

**CIAC**

Computer Incident Advisory Capability