Securing a Home Office/Small Office LAN

Gary C. Kessler
Champlain College
Gary Kessler Associates

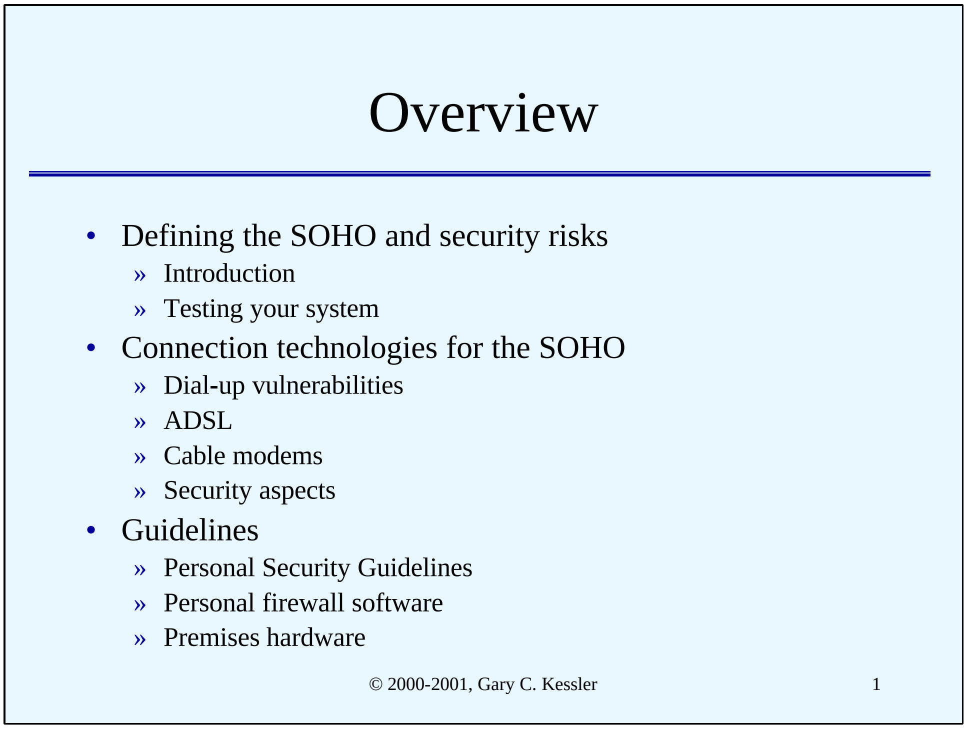
50 Creek Glen
Colchester, VT 05446
http://www.garykessler.net

kumquat@sover.net
+1 802-879-3375
+1 802-238-8913 (cell)
+1 630-604-5529 (fax)

Hi!

My name is Gary Kessler. I am an Assistant Professor at Champlain College in Burlington, VT and the program coordinator for the computer networking major. I am also an independent consultant working in the network security, TCP/IP, Internet, and e-commerce space.

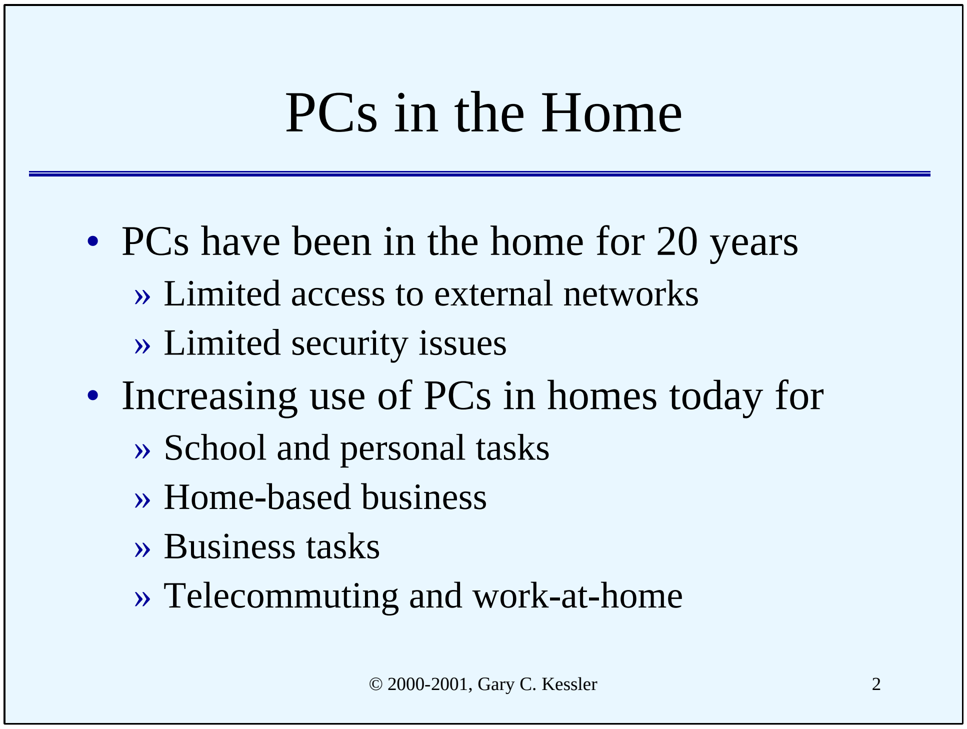
This session will discuss security aspects of home networks, or small office/home office (SOHO) networks, with particular attention to ADSL and cable modem access.



Overview

- Defining the SOHO and security risks
  - » Introduction
  - » Testing your system
- Connection technologies for the SOHO
  - » Dial-up vulnerabilities
  - » ADSL
  - » Cable modems
  - » Security aspects
- Guidelines
  - » Personal Security Guidelines
  - » Personal firewall software
  - » Premises hardware

This slide provides a basic outline of the topics that we will cover in this presentation.



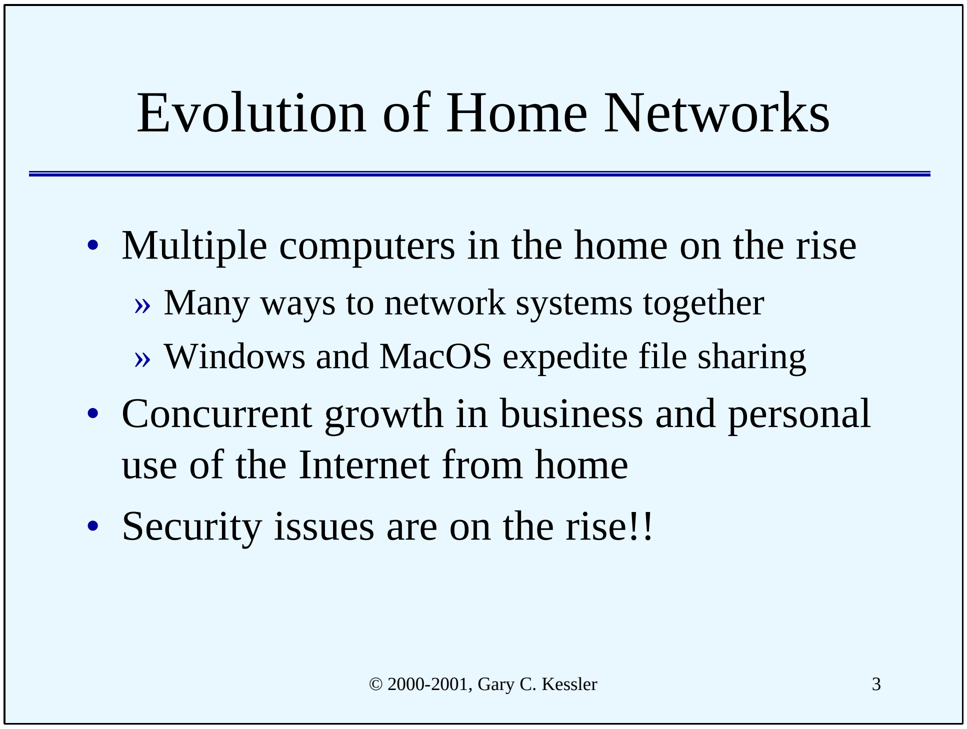
PCs in the Home

- PCs have been in the home for 20 years
  - » Limited access to external networks
  - » Limited security issues
- Increasing use of PCs in homes today for
  - » School and personal tasks
  - » Home-based business
  - » Business tasks
  - » Telecommuting and work-at-home

2

This slide and the next provide some deep background information. It is increasingly common today for families to have multiple computers in their home. But while PCs -- or PC-class machines -- have been around for over 20 years, cost was the main issue and security was not. My first PC-type machine was an Apple II+ purchased in 1981 for a cost somewhat above $2500. The Apple II+ was a great machine; 64 KB RAM (yes, KB), 2 floppy drives (hard drives for microcomputers didn't exist in 1981), about a 100-kHz CPU, a 300 bps modem, and a BASIC compiler. And that was a pretty good system!! But there was no Internet and a limited number of places to dial into such as the neighborhood Bulletin Board System (BBS) or some such. But there wasn't a big problem with other users attacking our computers.

Today, of course, PCs are everywhere. In particular, we have computers in the home for school work, business tasks (for both out-of-home and in-home businesses), and, increasingly, work-at-home and telecommuting applications. More and more of our personal information are on our computer -- medical information, personal finances, love letters, correspondence, e-mail, family photos, etc., etc. Our computer has become the repository of a larger set of personal items than we care to think.



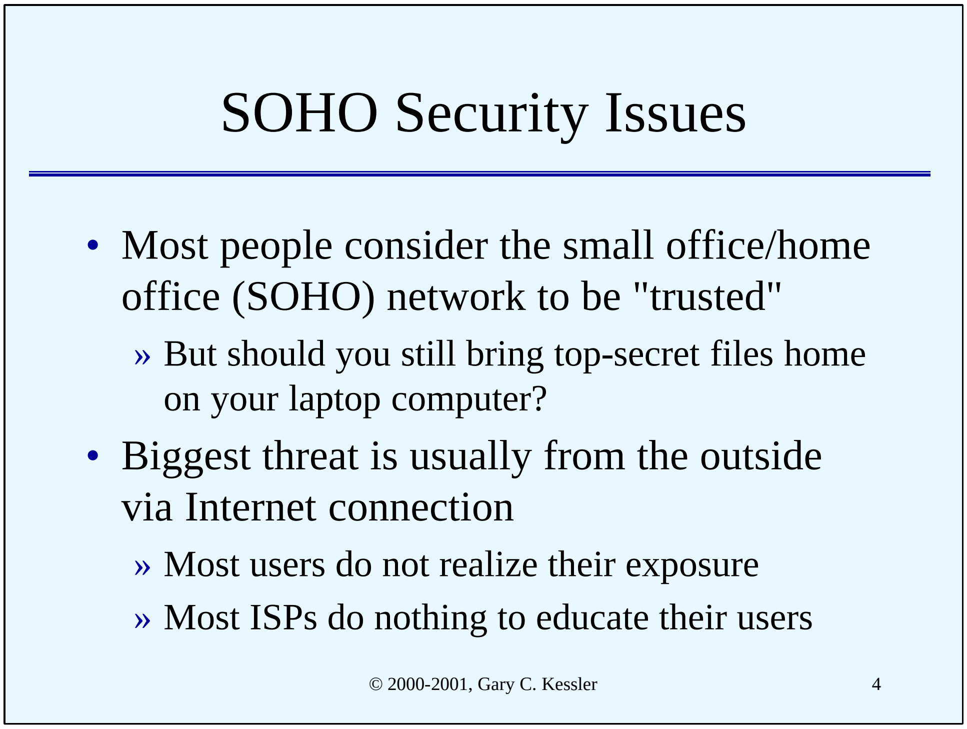
Evolution of Home Networks

- Multiple computers in the home on the rise
  - » Many ways to network systems together
  - » Windows and MacOS expedite file sharing
- Concurrent growth in business and personal use of the Internet from home
- Security issues are on the rise!!

With the price of computers dropping, the thought of getting more than one home computer is within the grasp of an increasing percentage of the population. Indeed, many of us have a laptop/notebook computer at work that we frequently bring home. For work, printer and file sharing, and backup purposes, a home network would be very handy. And with the price of network interface cards (NICs) and small hub/switch devices, the desire has become reality. Today's microcomputer operating systems -- Linux, MacOS, and Windows 3.11 et seq. – also make networking easy so that one doesn't even need additional software.

Couple the demand and simplicity for home networking with the growth in Internet use from the home for both personal and professional reasons, and we see the reason that there are more and more long-time (if not permanent) connections to the Internet.

And once on the Internet, security becomes an issue.



SOHO Security Issues

- Most people consider the small office/home office (SOHO) network to be "trusted"
  - » But should you still bring top-secret files home on your laptop computer?
- Biggest threat is usually from the outside via Internet connection
  - » Most users do not realize their exposure
  - » Most ISPs do nothing to educate their users

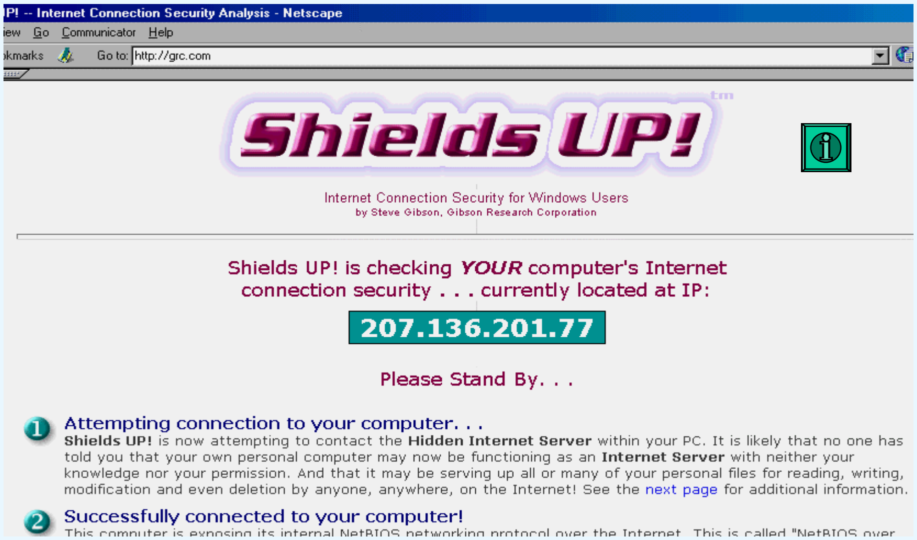
Most people don't consider the small office/home office (SOHO) environment to be a hostile one. And generally this is true. At home, I pretty much trust my spouse and children to not break in to my computer (why should they; they have access!).

But does this mean that I should bring home top secret files from the office on my laptop (as a former director of the CIA did)?

Indeed, the biggest threat that most of us face on our systems and networks at home *are* from the outside and because we don't focus on security at home. Most users, furthermore, don't recognize their exposure (nor their systems' vulnerabilities) on the 'Net. And Internet service providers (ISPs), for their part, don’t do enough to educate users, particularly when it comes to helping their users mitigate those exposures.

Sadly, most users just don't have a clue and the ISPs aren't helping them to get one!

Vulnerabilities On-line?



Internet Connection Security for Windows Users
by Steve Gibson, Gibson Research Corporation

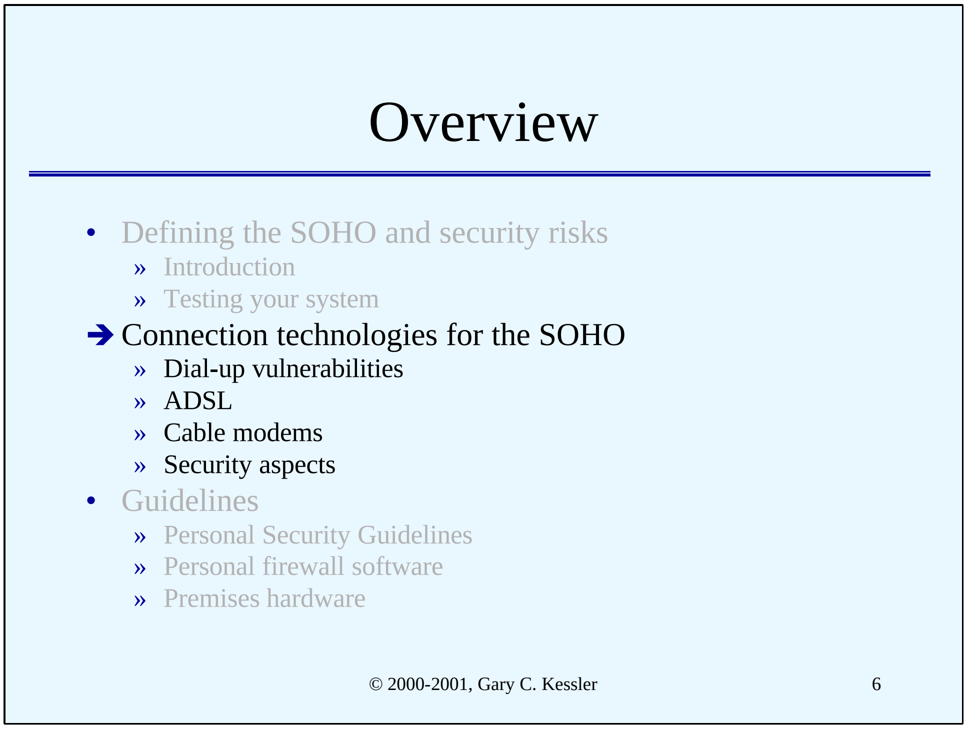
Shields UP! is checking ***YOUR*** computer's Internet connection security . . . currently located at IP:

207.136.201.77

Please Stand By. . .

1. Attempting connection to your computer. . .
   Shields UP! is now attempting to contact the **Hidden Internet Server** within your PC. It is likely that no one has told you that your own personal computer may now be functioning as an **Internet Server** with neither your knowledge nor your permission. And that it may be serving up all or many of your personal files for reading, writing, modification and even deletion by anyone, anywhere, on the Internet! See the next page for additional information.
2. Successfully connected to your computer!
   This computer is exposing its internal NetBIOS networking protocol over the Internet. This is called "NetBIOS over

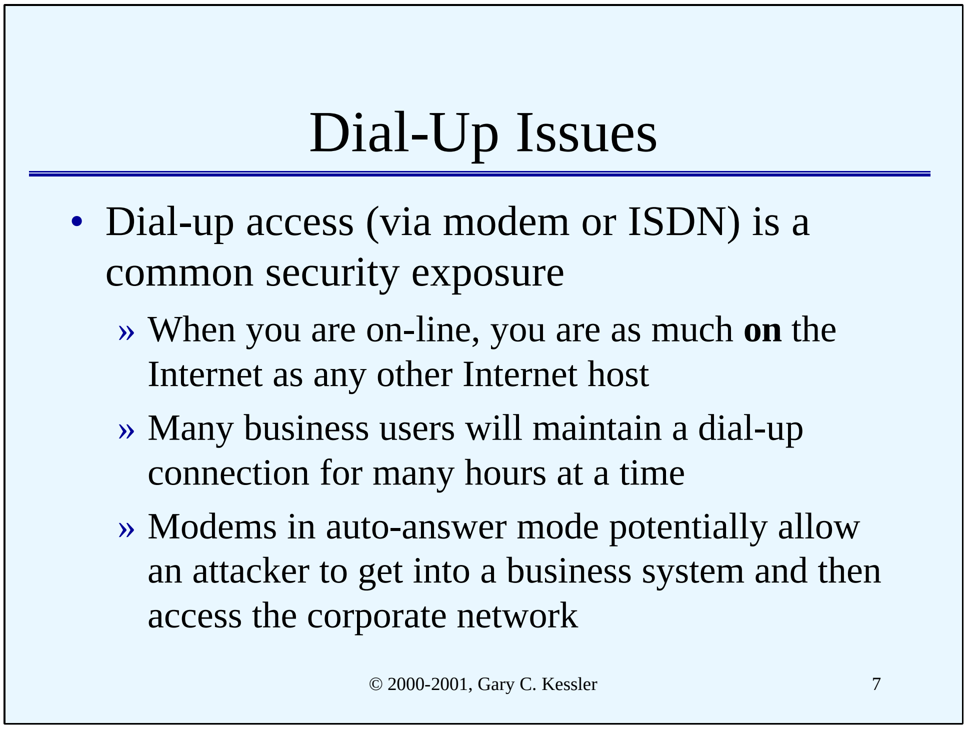
How vulnerable is your system when online? Check out *http://grc.com*, home of the Gibson Research Center. Use the opportunity to allow the ShieldsUP! software to test for NetBIOS weaknesses and scan your machine for open ports. If you have installed TCP/IP and accepted the default settings, and particularly if you have open shares, you might be amazed to see what ShieldsUP! can find out about your machine.



Overview

- Defining the SOHO and security risks
  - » Introduction
  - » Testing your system
- ➔ Connection technologies for the SOHO
  - » Dial-up vulnerabilities
  - » ADSL
  - » Cable modems
  - » Security aspects
- Guidelines
  - » Personal Security Guidelines
  - » Personal firewall software
  - » Premises hardware

This slide provides a basic outline of the topics that we will cover in this presentation.



Dial-Up Issues

- Dial-up access (via modem or ISDN) is a common security exposure
  - » When you are on-line, you are as much **on** the Internet as any other Internet host
  - » Many business users will maintain a dial-up connection for many hours at a time
  - » Modems in auto-answer mode potentially allow an attacker to get into a business system and then access the corporate network

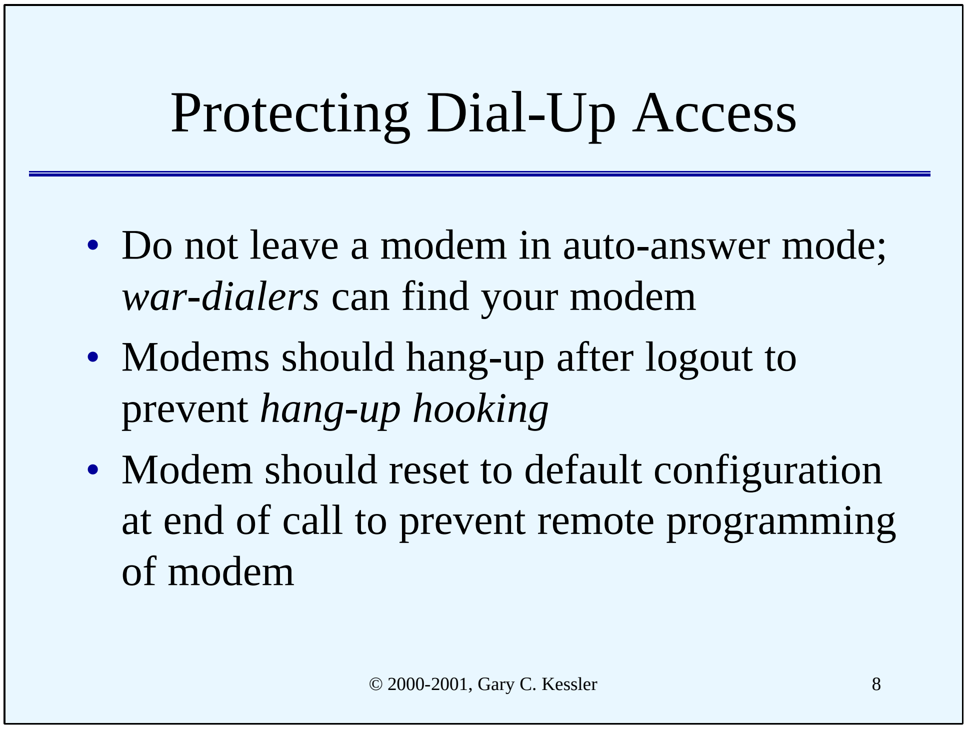
7

Let's start with analog or ISDN dial-up connections. Most people don't think that a computer with dial-up access has much security risk on the Internet because they're not on for that long a period of time. This is particularly true in those parts of the country where local calls are billed per-minute; in Vermont, for example, local access is billed at 2.2¢ per minute. But many telecommuters get on the Internet in the morning and stay on the line for hours at a time just to assure that they have a connection.

But regardless of the duration of the call, the point is that while you are connected to the Internet, your computer has an IP address and, therefore, has as much exposure to attackers and other bad people as any other host on the Internet. If a hacker is trolling for addresses and finds your's, a security exposure can still be exploited even if you're only on for a few minutes -- if it's the wrong few minutes!!

ISDN provides some protection if you drop the call during idle periods. The protection comes from the fact that an attacker can *not* initiate a connection back to your server if the ISDN connection isn't present. Of course, as soon as you're back on line, you're exposed again and many ISDN-connected customers have a permanently-assigned, static IP address.

Another exposure are environments where a PC has an auto-answer modem. In these cases, an attacker can make a connection to an unattended PC and access files on that machine or on other systems on the local network. Attackers might also be able to access a corporate network if the PC also has a dedicated network connection.



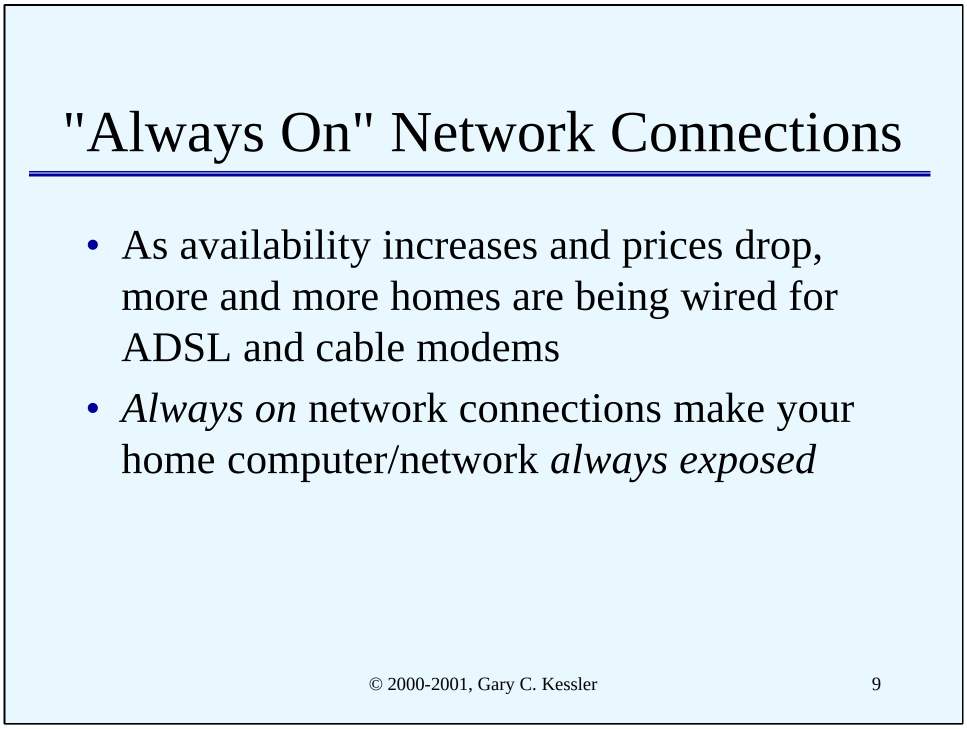
Protecting Dial-Up Access

- Do not leave a modem in auto-answer mode; *war-dialers* can find your modem
- Modems should hang-up after logout to prevent *hang-up hooking*
- Modem should reset to default configuration at end of call to prevent remote programming of modem

© 2000-2001, Gary C. Kessler 8

There are a few basic guidelines to protecting modems. They include:

1. Never leave a modem in auto-answer mode. If a modem needs to be in auto-answer mode (e.g., for field service calls), turn it on when it is needed and shut it off when it is not needed. If you require 24/7 auto-answer, be aware of the risk and isolate that computer if at all possible.
2. Modems should be configured to logout a user after the connection is dropped and to drop the connection after the user logs out. This prevents an attack known as *hang-up hooking* where an attacker actually causes an interruption in a valid user's connection and then quickly dials back to the modem on the same number and "continues" the interrupted session.
3. Configure the modem so that it resets to your site's default modem configuration at the end of each call. This prevents an attacker from connecting to the modem, changing the modem's settings, and dialing back in to take advantage of the changes.

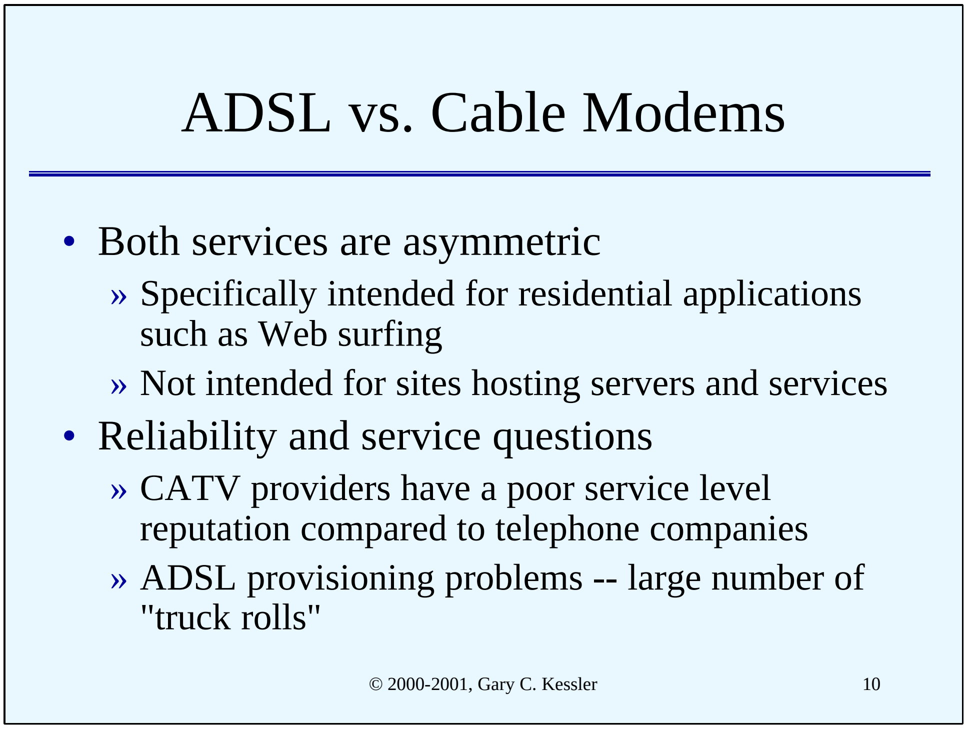


"Always On" Network Connections

- As availability increases and prices drop, more and more homes are being wired for ADSL and cable modems
- *Always on* network connections make your home computer/network *always exposed*

The cost of a conventional ISP account for unlimited dial-up access at speeds up to 56 kbps has been about $20/month in the U.S. for some time (this charge does not include any telephone charges). Always-on/always-connected ISP services using ADSL and cable modem access have been available since about 1999 and cost about $40-50/month *including* access. These latter services do not tie up a telephone line and, therefore, often pay for themselves. So in addition to getting hundreds of kbps in speed, users may be actually saving a few pennies.

But always-on has a hidden cost -- the user is now always exposed! Users who didn't pay no never mind to security when they had a modem didn't necessarily start thinking about in the 24/7 environment either.



ADSL vs. Cable Modems

- Both services are asymmetric
  - » Specifically intended for residential applications such as Web surfing
  - » Not intended for sites hosting servers and services
- Reliability and service questions
  - » CATV providers have a poor service level reputation compared to telephone companies
  - » ADSL provisioning problems -- large number of "truck rolls"

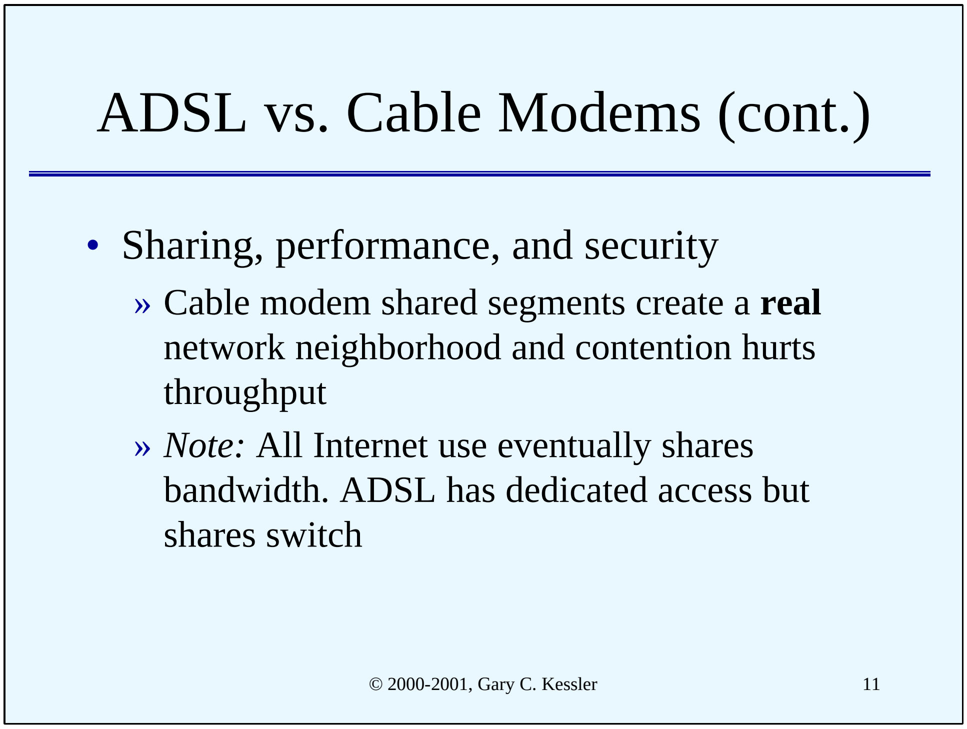
10

The ADSL and cable modem services have a number of things in common. First, both are asymmetric, offering a higher downstream data rate than upstream data rate. They are both intended as residential services to support typical residential applications, such as Web surfing and e-mail. (They're also well-suited to downloading MP3 files and more but that's another story!) In particular, ADSL and cable modem providers do not particularly want customers to hook up publicly accessible servers via these connections and, in fact, the asymmetric nature of the services make them poorly suited to server hosting applications.

Second, both services suffer from a perception -- or reality -- of poor service. Cable TV companies have long been maligned because of unexpected and frequent service outages, interference from sunspots (a phenomenon occurring 93 million miles away!), and generally poor quality plant and switches. How many times have cable companies around the U.S. been sued or fined by local municipalities or public service departments because of lack of performance or non-compliance with tariffs? In fairness, as the cable industry has consolidated, they have greatly improved the plant, noticeably improving service and "community citizenship."

Telephone companies are a different story. The Bell system in the U.S. has a 125 year history and their network is so reliable that maintaining it is considered essential to national security. So now let's talk about ADSL. The rollout of ADSL service in the U.S.has been plagued with difficulties. In many areas of the U.S., telcos have found a fairly small percentage of their local loops capable of supporting ADSL. Even where it is available, horror stories abound where multiple service calls from the telco (a "truck roll") are needed for successful service installation.

Another thing in common is the generally high customer satisfaction with both services *once they are successfully installed*.



ADSL vs. Cable Modems (cont.)

- Sharing, performance, and security
  - » Cable modem shared segments create a **real** network neighborhood and contention hurts throughput
  - » *Note:* All Internet use eventually shares bandwidth. ADSL has dedicated access but shares switch

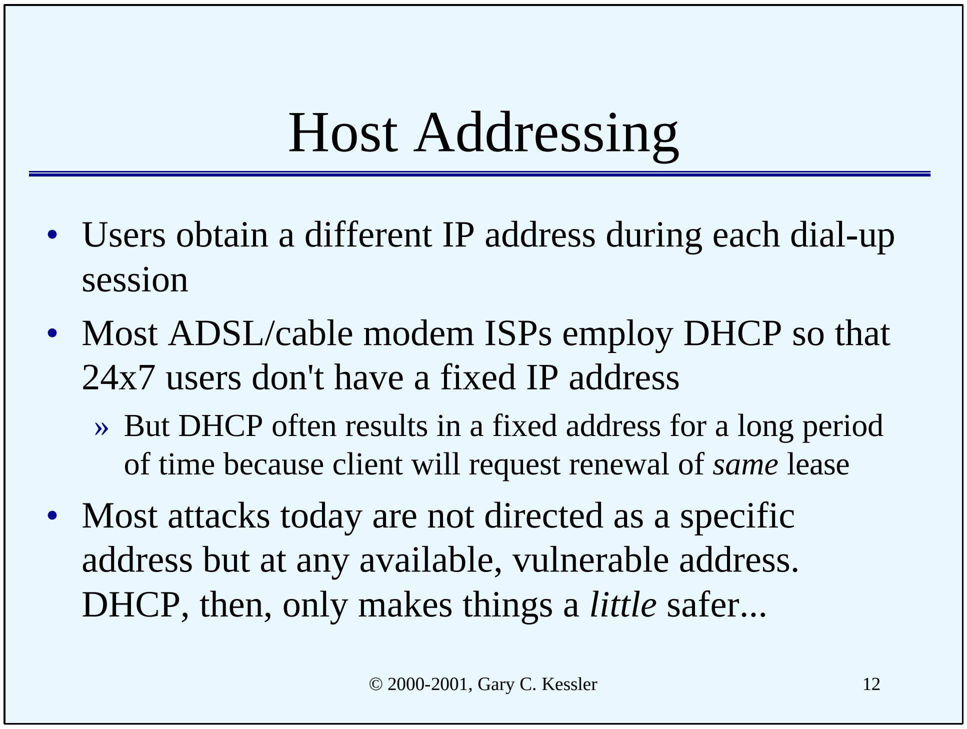
© 2000-2001, Gary C. Kessler 11

Cable modem services have been specifically vilified -- mostly by telcos! -- because their shared bandwidth results in additional security and performance issues that do not affect ADSL.

Let's start by reviewing the problem. In the cable modem network topology, customer premises that share a cable segment also share bandwidth; the service is a *shared medium* service for those customers, more or less analogous to the shared medium in a coax-based Ethernet LAN. ADSL, on the other hand, runs over the customer's point-to-point local loop back to the C.O. and, therefore, does not share bandwidth.

Well, sort of. In fact, all users on the Internet eventually share facilities and resources. It is absolutely correct that all premises in a neighborhood share a cable segment in the cable modem model. But while ADSL users own the wire, they share the capacity of the DSLAM in the C.O. Why does this matter? Because a well-engineered cable modem network will provide adequate service while a poorly-engineered DSLAM will suffer poor performance. The point -- a well-engineered service will do fine; bandwidth contention on a cable modem network as a root of bad performance compared to ADSL is a red herring.

What is much more of a real problem is security. Indeed, the shared nature of cable modem services makes the potential security problems very real; browsing the network neighborhood can take on whole new meaning if every house on the block shares a cable! We'll address that issue in upcoming slides.



Host Addressing

- Users obtain a different IP address during each dial-up session
- Most ADSL/cable modem ISPs employ DHCP so that 24x7 users don't have a fixed IP address
  - » But DHCP often results in a fixed address for a long period of time because client will request renewal of *same* lease
- Most attacks today are not directed as a specific address but at any available, vulnerable address. DHCP, then, only makes things a *little* safer...

12

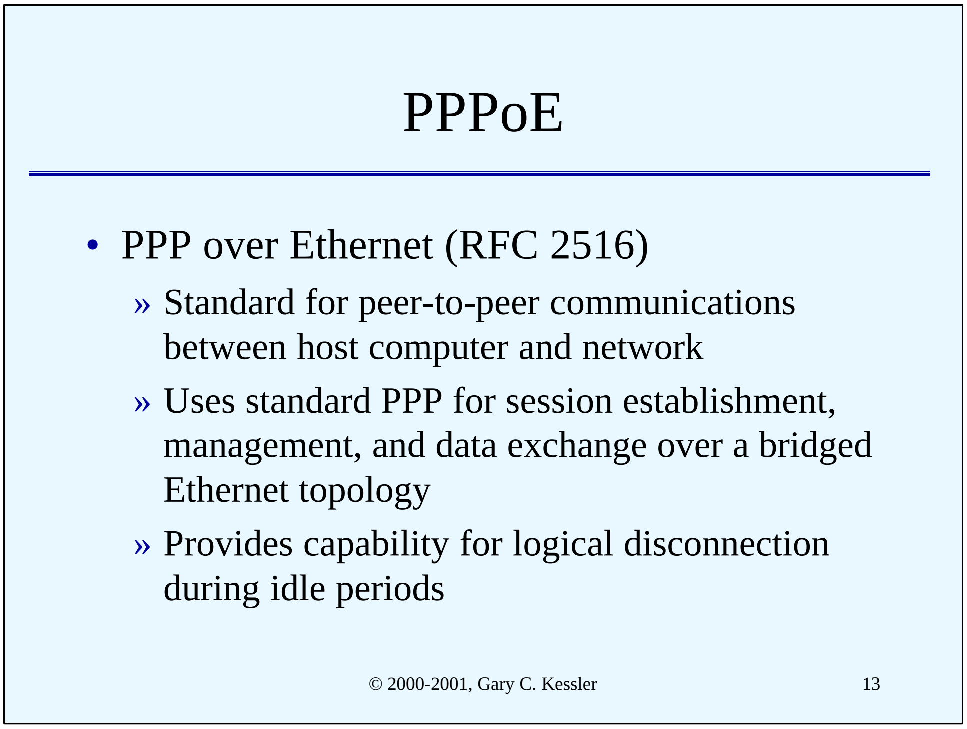
In earlier discussion, we mentioned that when your PC or host is attached to the Internet, it has an IP address and is as accessible as any other host on the Internet.

In the dial-up environment, a user receives a different IP address every time they dial up to their ISP. This certainly helps prevent a given host from being targeted by an attacker.

To provide the same protection for 24/7 connections, ADSL and cable modem providers generally employ the Dynamic Host Configuration Protocol (DHCP) to dynamically assign IP addresses to customers. Some service providers purposely terminate the IP address lease frequently; others end up renewing the lease over and over so that a host maintains the same IP address for a long period of time.

Service providers really use DHCP for a couple of reasons, one of which is to help protect users. But of even more significance to the providers is that it makes it difficult for the customer to try to run a server on the premises; if the IP address of the server changes frequently, it becomes hard to advertise and most bona fide companies want a real, permanent host name and IP address to out in the Domain Name System (DNS) database.

Note that DHCP still only helps a little. Most attacks on systems connected to the Internet via dial-up, ADSL, or cable modem are *not* directed at the victim host; indeed, the host was found by someone trolling for pingable IP addresses within some range of addresses.



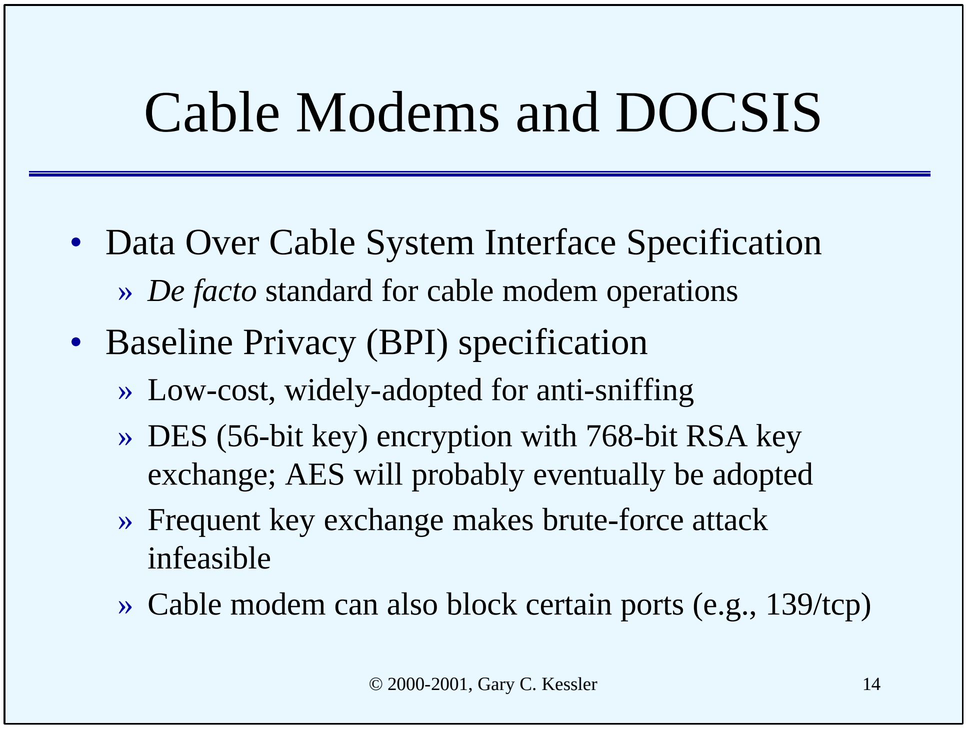
PPPoE

- PPP over Ethernet (RFC 2516)
  - » Standard for peer-to-peer communications between host computer and network
  - » Uses standard PPP for session establishment, management, and data exchange over a bridged Ethernet topology
  - » Provides capability for logical disconnection during idle periods

13

Request for Comments (RFC) 2516 describes a protocol called the Point-to-Point Protocol over Ethernet (PPPoE). Designed specifically for ADSL, PPPoE defines a way to encapsulate an IP packet in a PPP frame that is transported over the Ethernet protocol. The general idea of PPPoE is to be able to extend an Ethernet network logically across bridging devices such as the ADSL modem and telco's access concentrator. It also provides a mechanism to logically disconnect a host from the Internet during periods of idleness; this is the best protection that a provider can offer a customer. When the user points the browser to a URL or when the user's e-mail client tries to access the Internet to check mail, PPP procedures re-establish the logical connection. This entire operation is fast because the physical connection is still intact and is transparent to the end user.

RFC 2516 can be found at *ftp://ftp.isi.edu/in-notesrfc2516.txt* or via the RFC Editor's Web site *(http://www.rfc-editor.org*).



Cable Modems and DOCSIS

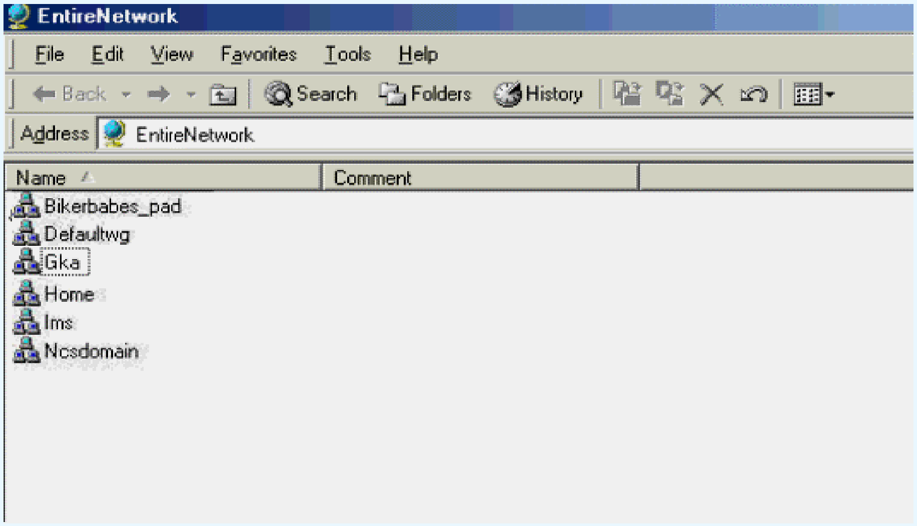
- Data Over Cable System Interface Specification
  - *De facto* standard for cable modem operations
- Baseline Privacy (BPI) specification
  - Low-cost, widely-adopted for anti-sniffing
  - DES (56-bit key) encryption with 768-bit RSA key exchange; AES will probably eventually be adopted
  - Frequent key exchange makes brute-force attack infeasible
  - Cable modem can also block certain ports (e.g., 139/tcp)

The Data Over Cable System Interface Specification (DOCSIS) is the cable TV industry's *de facto* standard for deploying and operating a cable modem Internet access service. One of the lesser known aspects of DOCSIS is the Baseline Privacy (BPI) specification. This is a low-cost and widely-deployed scheme that provides protection from neighborhood packet sniffing and NetBIOS browsing.

To prevent someone from sniffing packets on the cable, BPI specifies the use of 56-bit DES encryption between the cable modem and head-end. Although DES is clearly not the strongest of crypto schemes, the DES key is changed frequently to make a brute force attack infeasible; it is unlikely that someone will buffer all of your packets and try to break the key if the key is changed daily. Secret key exchange is performed using 768-bit RSA. It is likely that the new AES specification will be employed (after it is formally adopted) in the next release of BPI.

BPI also specifies that certain "dangerous" TCP/UDP ports be blocked, particularly TCP port 139 (NetBIOS session service); blocking 139/tcp makes file and print sharing impossible. Some cable modems also allow blocking of other routable networking protocols, such as AppleTalk and Novell NetWare's Internetwork Packet Exchange (IPX).

Browsing the Neighborhood (1)

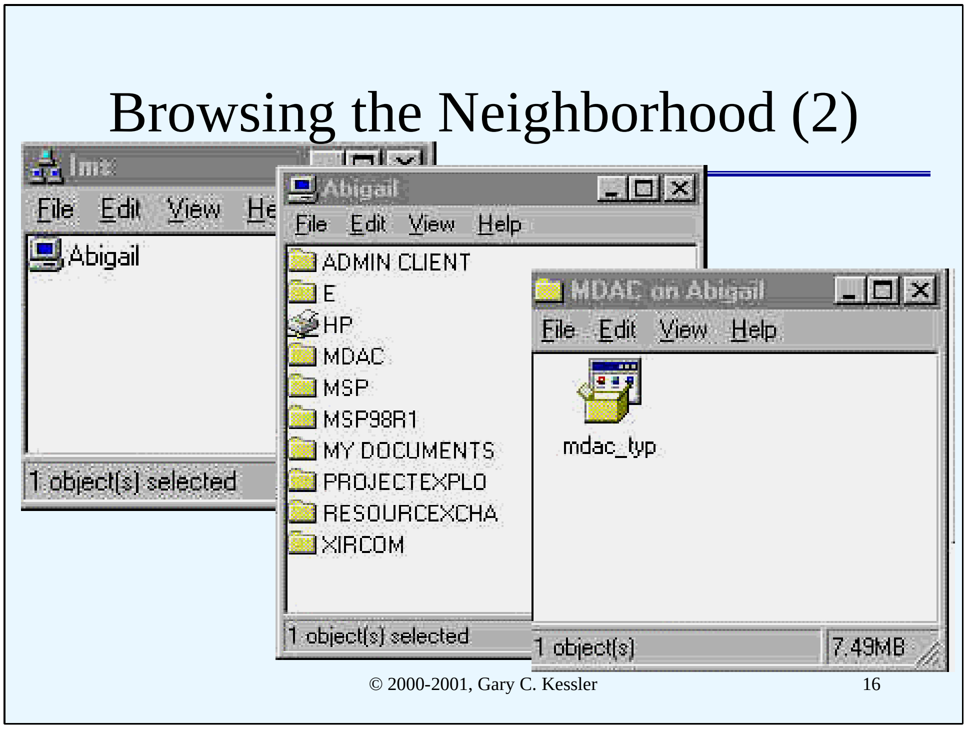


Name	Comment
Bikerbabes_pad	
Defaultwg	
Gka	
Home	
Ims	
Ncsdomain	

15

This slide and the next two show an example of what can happen on a cable network where the provider does not supply cable modems that block file and print sharing *and* customers don't protect themselves. While these graphics have been somewhat sanitized, the scenario is real.

In this slide, a user connected to the cable modem uses Windows' Network Neighborhood capability and finds... a lot of domains and workgroups that are not the user's!



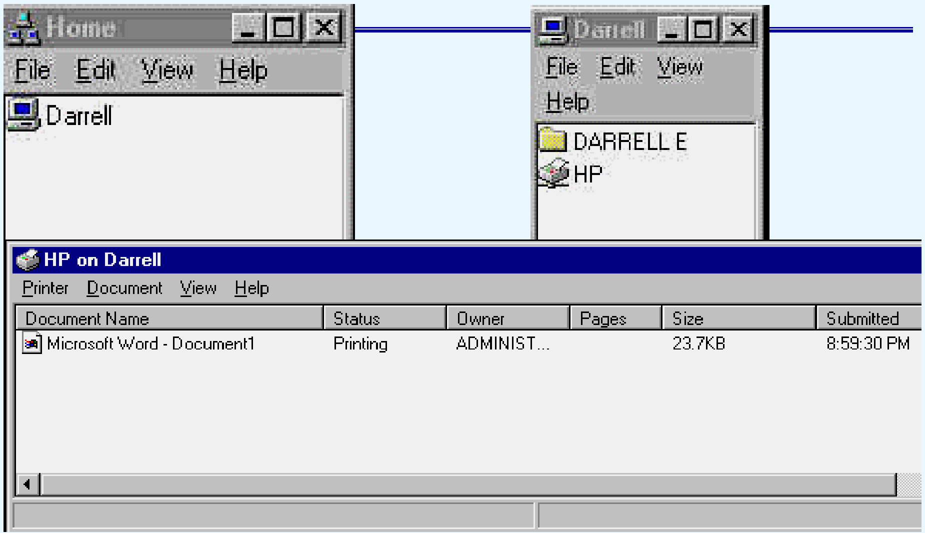
Browsing the Neighborhood (2)

© 2000-2001, Gary C. Kessler 16

One of the workgroups that appeared in Network Neighborhood is called Ims. Expanding Ims brings up the window shown on the left, containing a computer named Abigail.

Expanding Abigail brings up the window shown in the middle, containing a number of NetBIOS *shares*: ten directories (folders) and a printer called HP. Expanding the MDAC share brings up the window on the right, containing a file called *mdac_typ.exe*. Not shown here is dragging the file *mdac_typ.exe* to the computer displaying these windows.

Browsing the Neighborhood (3)



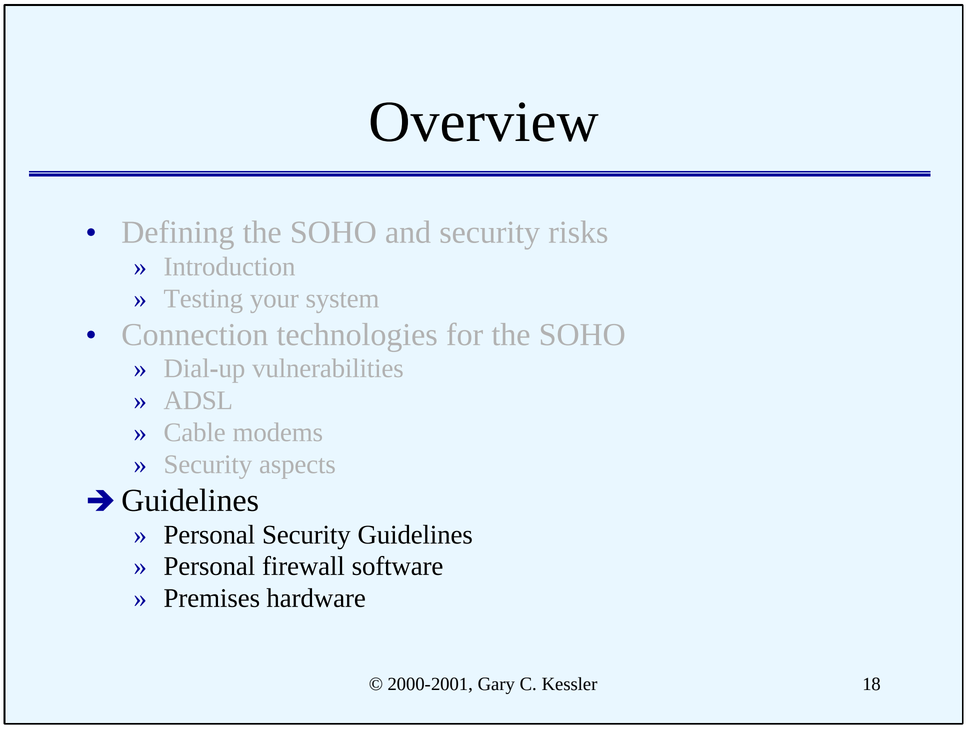
Document Name	Status	Owner	Pages	Size	Submitted
Microsoft Word - Document1	Printing	ADMINIST...		23.7KB	8:59:30 PM

One of the workgroups that appeared in Network Neighborhood is called Home. Expanding Home brings up the window shown in the upper-left, containing a computer named Darrell.

Expanding Darrell brings up the window on the upper-right, showing two *shares*: the directory (folder) called DARRELL E and a printer called HP.

Expanding the HP share shows the status of the printer queue, which has a currently printing job.

What is not shown here is the fact that upon finding the HP printer share, the person who generated these screen shots loaded a generic HP driver onto their computer and then directed a print job to the printer. *That* is the print job currently printing on the remote computer.

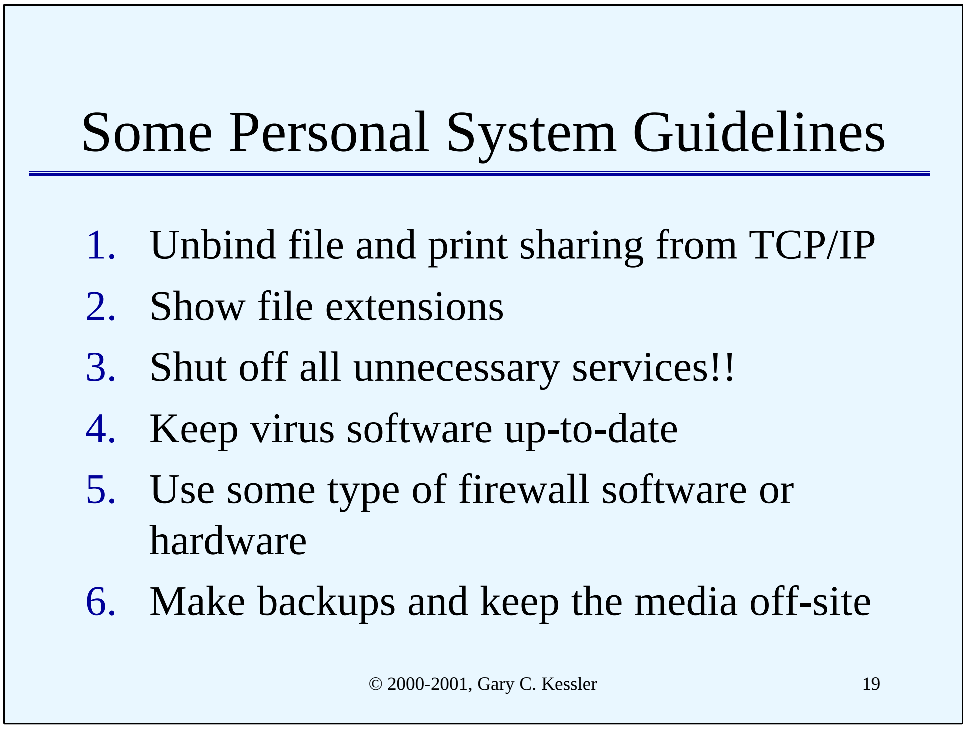


Overview

- Defining the SOHO and security risks
  - » Introduction
  - » Testing your system
- Connection technologies for the SOHO
  - » Dial-up vulnerabilities
  - » ADSL
  - » Cable modems
  - » Security aspects
- ➔ Guidelines
  - » Personal Security Guidelines
  - » Personal firewall software
  - » Premises hardware

18

This slide provides a basic outline of the topics that we will cover in this presentation.



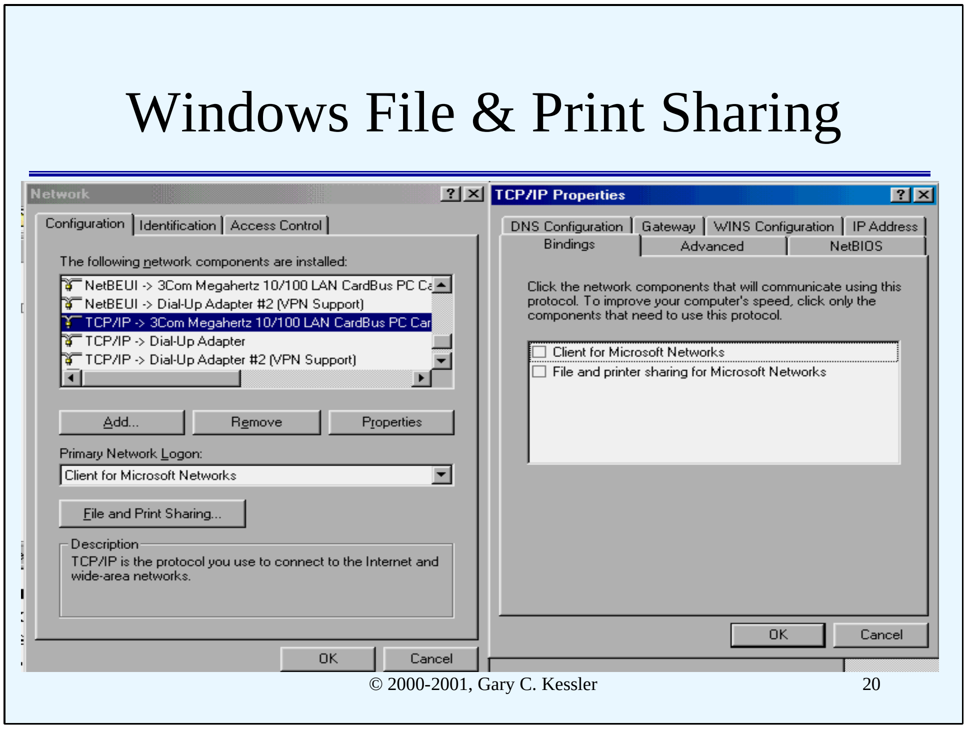
Some Personal System Guidelines

1. Unbind file and print sharing from TCP/IP
2. Show file extensions
3. Shut off all unnecessary services!!
4. Keep virus software up-to-date
5. Use some type of firewall software or hardware
6. Make backups and keep the media off-site

© 2000-2001, Gary C. Kessler 19

There are a number of actions that a user can take to protect themselves when on the Internet, either via dial-up or 24/7 (ADSL or cable modem) access:

1. Windows users should disassociate (unbind) file and print sharing from TCP/IP. Details on how to accomplish this are provided on the next page.
2. Another hint for Windows users: display file extensions, an option that is *off* by default. When the Anna Kournikova virus hit on 2/12/2001, for example, many people opened the virus file, named *annakournikova.jpg.vbs*, because all they saw was *annakournikova.jpg* and they thought it was a "safe" JPEG file. Display file extensions by opening Windows Explorer, choose the View, Folder Options... submenu, and click on the View tab.
3. All unnecessary or unused services should be turned off on your computer. Details on this are provided on later pages.
4. Virus software should be installed on your computer and always running. In addition, you should regularly (at least weekly!) check for new anti-virus signature files from your anti-virus software vendor.
5. Employ some sort of software and/or hardware firewall for your connection. Both types of firewall will be discussed on later pages.
6. Make backups of your computer files. At the very least, backup all files with volatile data, such as program source code, word processing documents, presentations, Web pages, your Quicken database, etc. Be sure that you have a backup of your installed software, as well; it is actually sometimes easier to reinstall software and recover data files than to try to rebuild the entire system. Also, know your reason for doing a backup and plan for the disaster for which you are trying to recover. If you are worried only about disk failure, a second disk drive might be sufficient for backup; if you are also worried about fire or flood, be sure to store your backup media offsite.



Windows File & Print Sharing

The following network components are installed:

- NetBEUI -> 3Com Megahertz 10/100 LAN CardBus PC Ca
- NetBEUI -> Dial-Up Adapter #2 (VPN Support)
- TCP/IP -> 3Com Megahertz 10/100 LAN CardBus PC Car
- TCP/IP -> Dial-Up Adapter
- TCP/IP -> Dial-Up Adapter #2 (VPN Support)

Primary Network Logon: Client for Microsoft Networks

Description
TCP/IP is the protocol you use to connect to the Internet and wide-area networks.

Click the network components that will communicate using this protocol. To improve your computer's speed, click only the components that need to use this protocol.

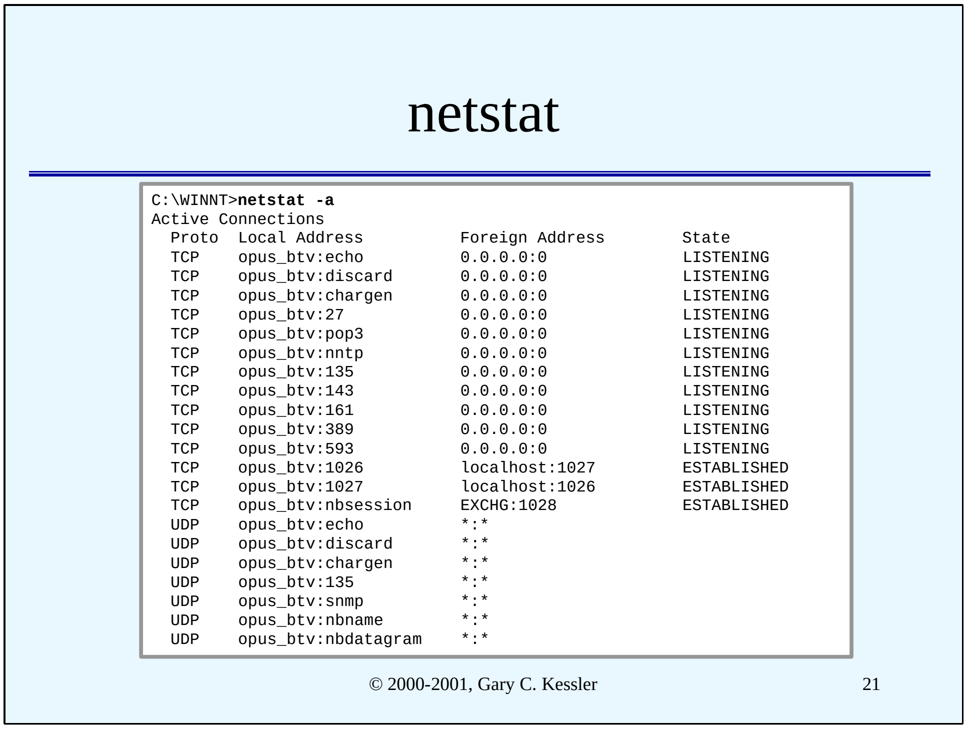
□ Client for Microsoft Networks
□ File and printer sharing for Microsoft Networks

20

Windows computers are particularly vulnerable to attack because file and print sharing is, by default, enabled and bound to TCP/IP when TCP/IP is installed. That means that the following ports are open and listening:

- UDP port 137, nbname (NetBIOS name service)
- UDP port 138, nbdatagram (NetBIOS datagram service)
- TCP port 139, nbsession (NetBIOS session service)

This setting is unnecessary and dangerous. Before getting connected in any way to the Internet, Windows users should block file and print sharing over TCP/IP. This is simply accomplished; as shown in the slide, go into the Network configuration under Control Panel, and unbind "Client for Microsoft Networks" and "File and print sharing for Microsoft Networks" in the TCP/IP properties for all adapters using TCP/IP. You can still do all of the file and print sharing that you want over the LAN because Microsoft networks use the NetBIOS protocol and don't need to have these functions bound to TCP/IP.



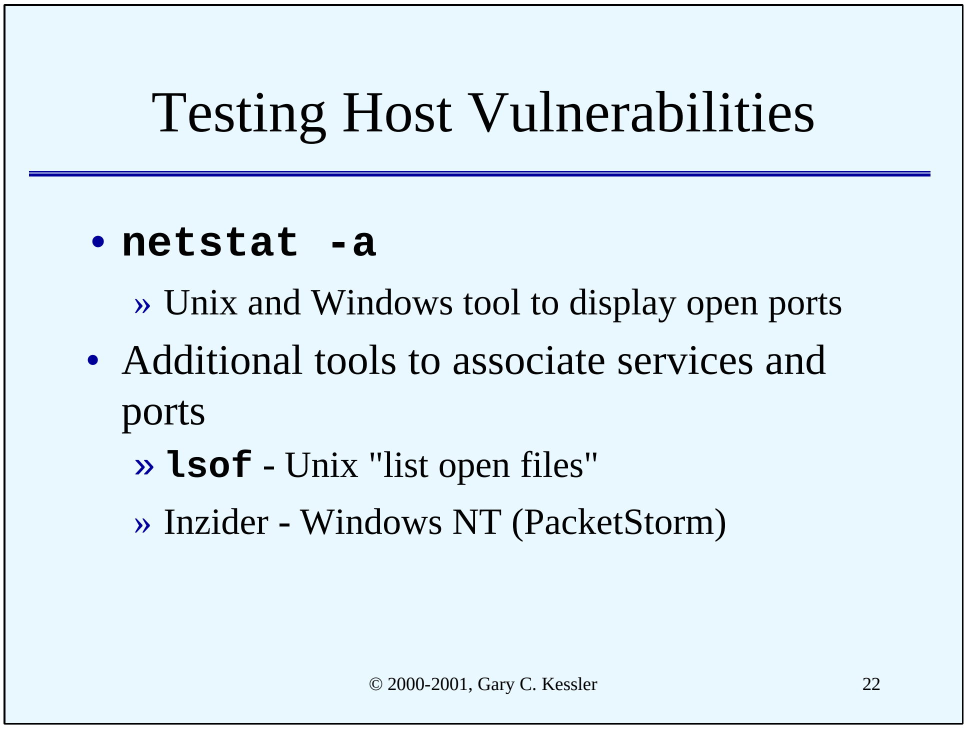
netstat

```
C:\WINNT>netstat -a
Active Connections
  Proto  Local Address          Foreign Address        State
  TCP    opus_btv:echo          0.0.0.0:0              LISTENING
  TCP    opus_btv:discard       0.0.0.0:0              LISTENING
  TCP    opus_btv:chargen       0.0.0.0:0              LISTENING
  TCP    opus_btv:27            0.0.0.0:0              LISTENING
  TCP    opus_btv:pop3          0.0.0.0:0              LISTENING
  TCP    opus_btv:nntp          0.0.0.0:0              LISTENING
  TCP    opus_btv:135           0.0.0.0:0              LISTENING
  TCP    opus_btv:143           0.0.0.0:0              LISTENING
  TCP    opus_btv:161           0.0.0.0:0              LISTENING
  TCP    opus_btv:389           0.0.0.0:0              LISTENING
  TCP    opus_btv:593           0.0.0.0:0              LISTENING
  TCP    opus_btv:1026          localhost:1027         ESTABLISHED
  TCP    opus_btv:1027          localhost:1026         ESTABLISHED
  TCP    opus_btv:nbsession     EXCHG:1028             ESTABLISHED
  UDP    opus_btv:echo          *:*
  UDP    opus_btv:discard       *:*
  UDP    opus_btv:chargen       *:*
  UDP    opus_btv:135           *:*
  UDP    opus_btv:snmp          *:*
  UDP    opus_btv:nbname        *:*
  UDP    opus_btv:nbdatagram    *:*
```

On all systems, it is important to know what services are running and, in particular, on what TCP and UDP ports your computer is LISTENING, or possibly willing to accept an attachment from the outside.

The basic tool used to determine which ports are open is `netstat -a`, available in both Unix and Windows (DOS); the slide shows such a command issued on a Windows NT Server system. Ideally, no ports should be open except ones that you expect.

Windows NT is particularly interesting; note all of the open ports that are on by default on this Exchange (e-mail) Server. What is the purpose of the echo, discard, and character generator (chargen) services, for example?



Testing Host Vulnerabilities

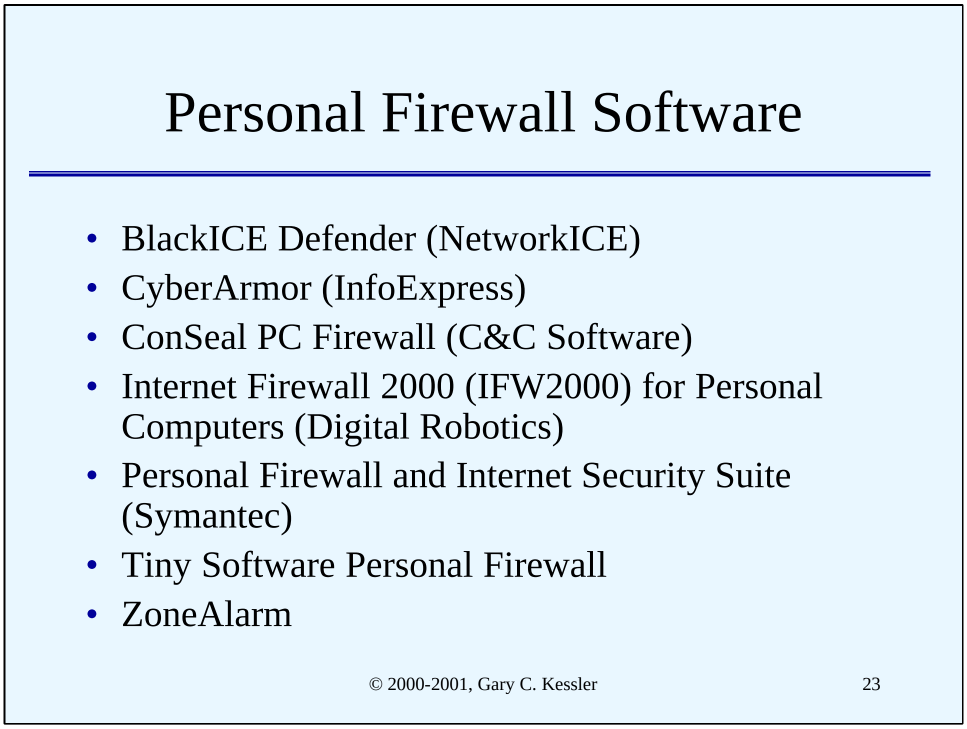
- `netstat -a`
  - Unix and Windows tool to display open ports
- Additional tools to associate services and ports
  - `lsof` - Unix "list open files"
  - Inzider - Windows NT (PacketStorm)

22

While `netstat` tells you which ports on your computer are LISTENING, it will not tell you what services are associated with those ports and that can make shutting the ports harder. There are additional tools that you can use to determine what application is running what Internet service:

• `lsof` is the "list open files" command available in Unix

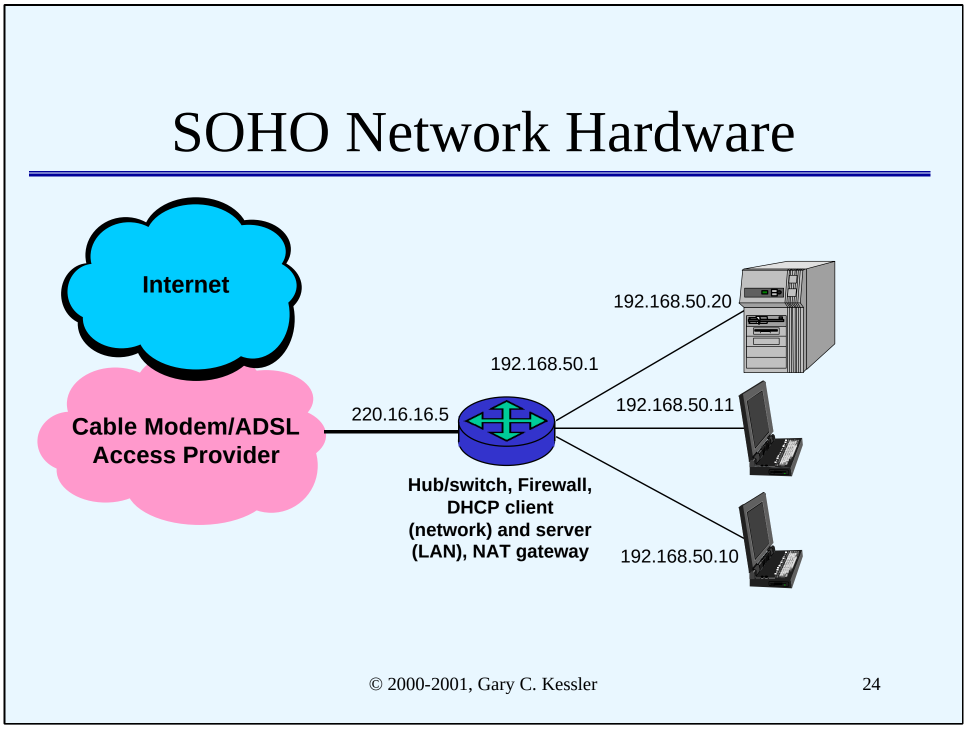
• *Inzider* is a 3rd-party software for Windows NT that is available from PacketStorm (*http://packetstorm.securify.com*)



Personal Firewall Software

- BlackICE Defender (NetworkICE)
- CyberArmor (InfoExpress)
- ConSeal PC Firewall (C&C Software)
- Internet Firewall 2000 (IFW2000) for Personal Computers (Digital Robotics)
- Personal Firewall and Internet Security Suite (Symantec)
- Tiny Software Personal Firewall
- ZoneAlarm

Personal firewall software is one important tool to protect computers in the SOHO environment. This slide lists several products with a range of features and capabilities, ranging in price from free to US$70.

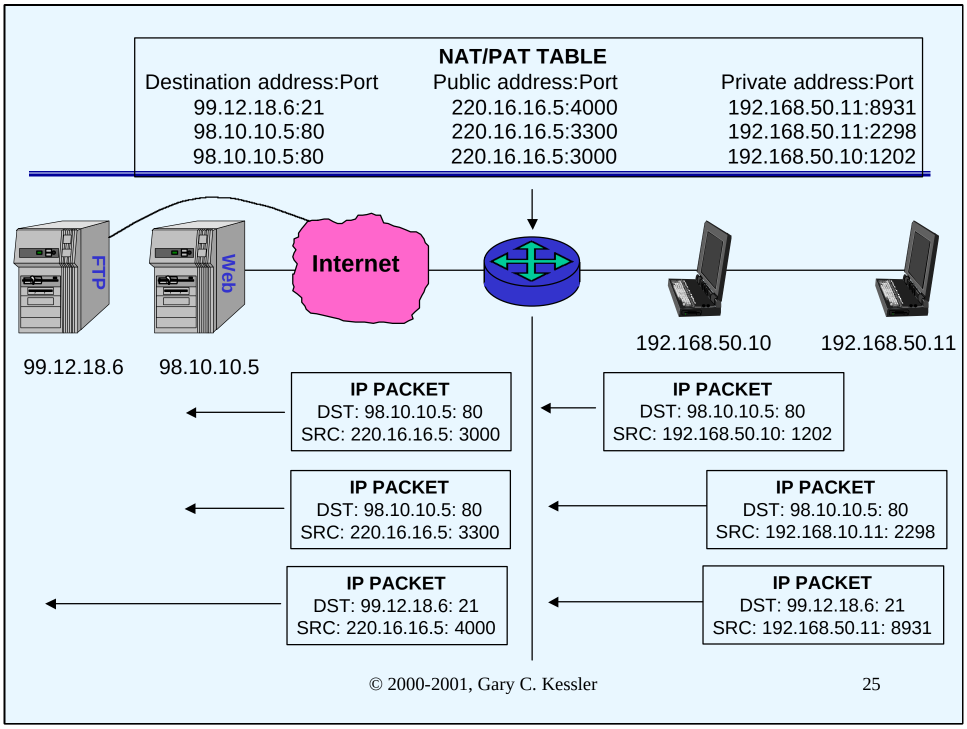


SOHO Network Hardware

Internet
Cable Modem/ADSL Access Provider
220.16.16.5
192.168.50.1
Hub/switch, Firewall, DHCP client (network) and server (LAN), NAT gateway
192.168.50.20
192.168.50.11
192.168.50.10

Increasingly, residential and SOHO sites do not have a single system connected to the Internet but a LAN that they want connected to the Internet. But since these are "residential" services, the site is only provided with a single IP address, and only temporarily at that.

A new set of products has emerged to meet the requirements of home/SOHO networks, as shown in the slide. In this example, the site has been assigned the public IP address 220.16.16.5. But instead of connecting the ADSL or cable modem directly to a single PC, it is attached to small router that looks like a Dynamic Host Configuration Protocol (DHCP) client to the network and acts like a firewall to the LAN. In this case, we will use the RFC 1918 private IP network number 192.168.50.0; the router, then, has to be able to perform Network Address Translation (NAT) to map the private host addresses to the single public address. The router might also be able to act like a DHCP server for the LAN and may even include an embedded LAN hub or switch.



NAT/PAT TABLE

Destination address:Port	Public address:Port	Private address:Port
99.12.18.6:21	220.16.16.5:4000	192.168.50.11:8931
98.10.10.5:80	220.16.16.5:3300	192.168.50.11:2298
98.10.10.5:80	220.16.16.5:3000	192.168.50.10:1202

IP PACKET
DST: 98.10.10.5: 80
SRC: 220.16.16.5: 3000

IP PACKET
DST: 98.10.10.5: 80
SRC: 192.168.50.10: 1202

IP PACKET
DST: 98.10.10.5: 80
SRC: 220.16.16.5: 3300

IP PACKET
DST: 98.10.10.5: 80
SRC: 192.168.10.11: 2298

IP PACKET
DST: 99.12.18.6: 21
SRC: 220.16.16.5: 4000

IP PACKET
DST: 99.12.18.6: 21
SRC: 192.168.50.11: 8931

25

NAT is one of the most important features of a home/SOHO router. Because there is only a single public IP address, all hosts share that one address and do *port address translation* (PAT) (or *network address port translation*, NAPT) to make all of the network connections unambiguous. This conserves IP addresses and also provides good security for the premises systems.

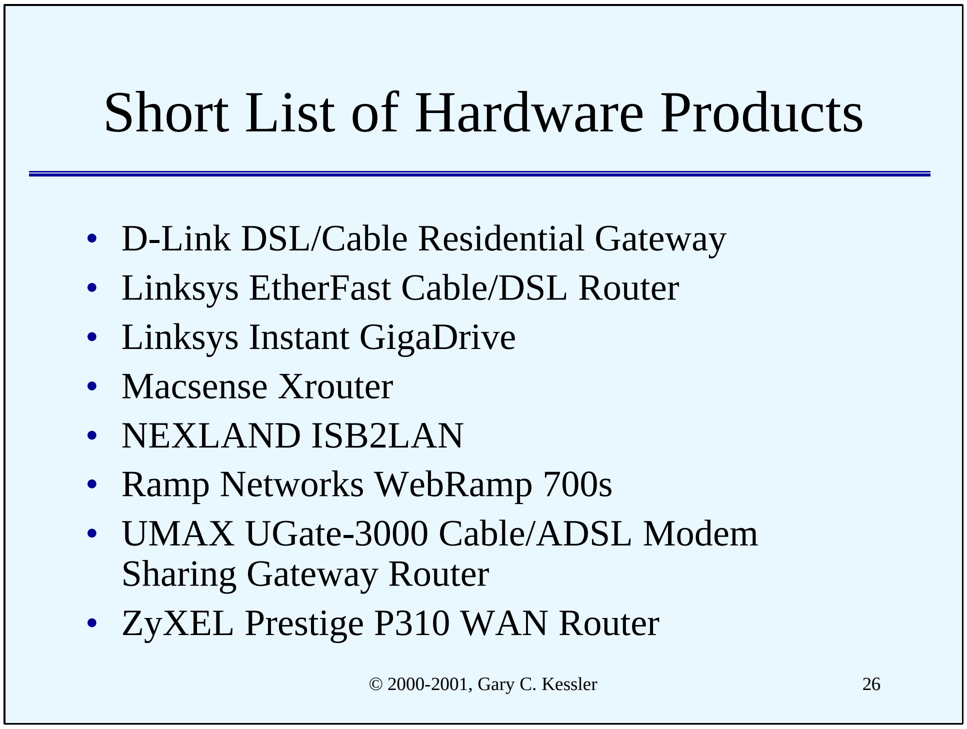
Consider the example in the slide. There are two local hosts (with the private addresses 192.168.50.10 and 192.168.50.11) that share the public address 220.16.16.5. These hosts will make a connection to the FTP and Web servers on the Internet, as shown.

1. Host 192.168.50.10 connects to the Web server (destination port 80) at 98.10.10.5. In the packet that is generated, the source port is chosen to be 1202. When this packet gets to the router providing NAT, the router changes the packet's source address to 220.16.16.5 and the source port to 3000.

2. Host 192.168.50.11 now connects to the Web server at 98.10.10.5, using a source port number of 2298. When this packet gets to the NAT router, a new table entry is made and the router changes the packet's source address to the shared public address 220.16.16.5 and the source port becomes 3300.

3. Host 192.168.50.11 now connects to the FTP server (destination port 21) at 99.12.18.6, using a source port number of 8931. When this packet gets to the NAT router, the packet's source address is again 220.16.16.5 and the source port becomes 4000.

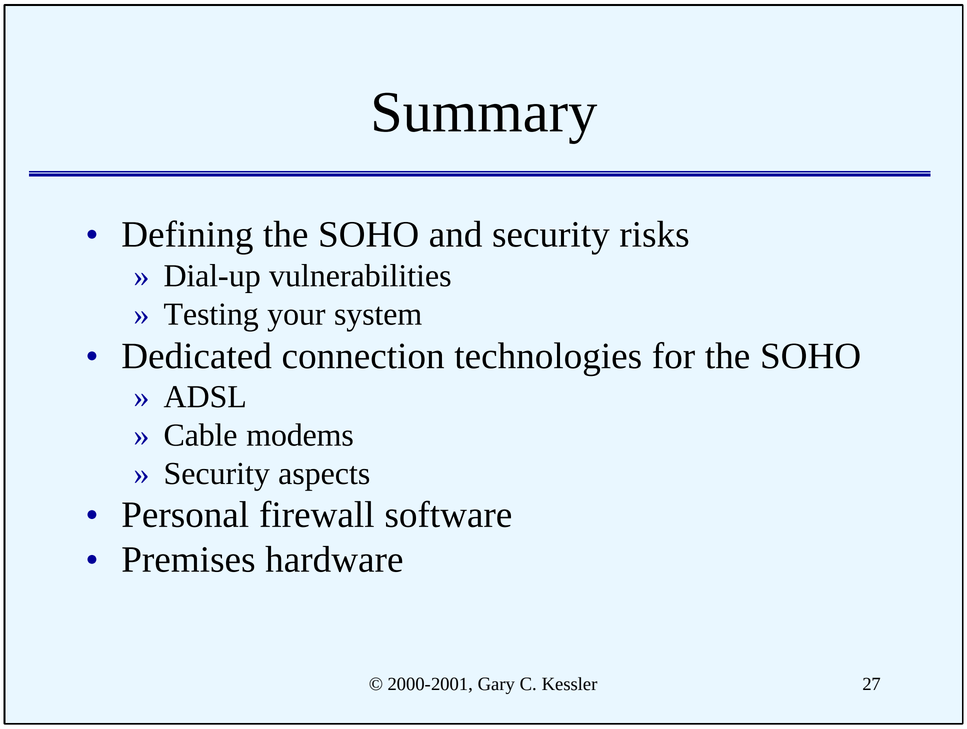
The point of this slide, of course, is to show how the three connections between the two local client systems and two servers can be accomplished even when using a single IP address. Use of port address translation essentially extends the size of the address space. And conceptually, this is the way in which a single host would distinguish between three Internet connections to multiple destinations.



Short List of Hardware Products

- D-Link DSL/Cable Residential Gateway
- Linksys EtherFast Cable/DSL Router
- Linksys Instant GigaDrive
- Macsense Xrouter
- NEXLAND ISB2LAN
- Ramp Networks WebRamp 700s
- UMAX UGate-3000 Cable/ADSL Modem Sharing Gateway Router
- ZyXEL Prestige P310 WAN Router

This slide lists several of hardware products that provide the features described on the last two pages. These products have a range of features and capabilities, ranging in price from US$150 to US$400.



Summary

- Defining the SOHO and security risks
  - » Dial-up vulnerabilities
  - » Testing your system
- Dedicated connection technologies for the SOHO
  - » ADSL
  - » Cable modems
  - » Security aspects
- Personal firewall software
- Premises hardware

For more information, please refer to the contact information on the first slide.