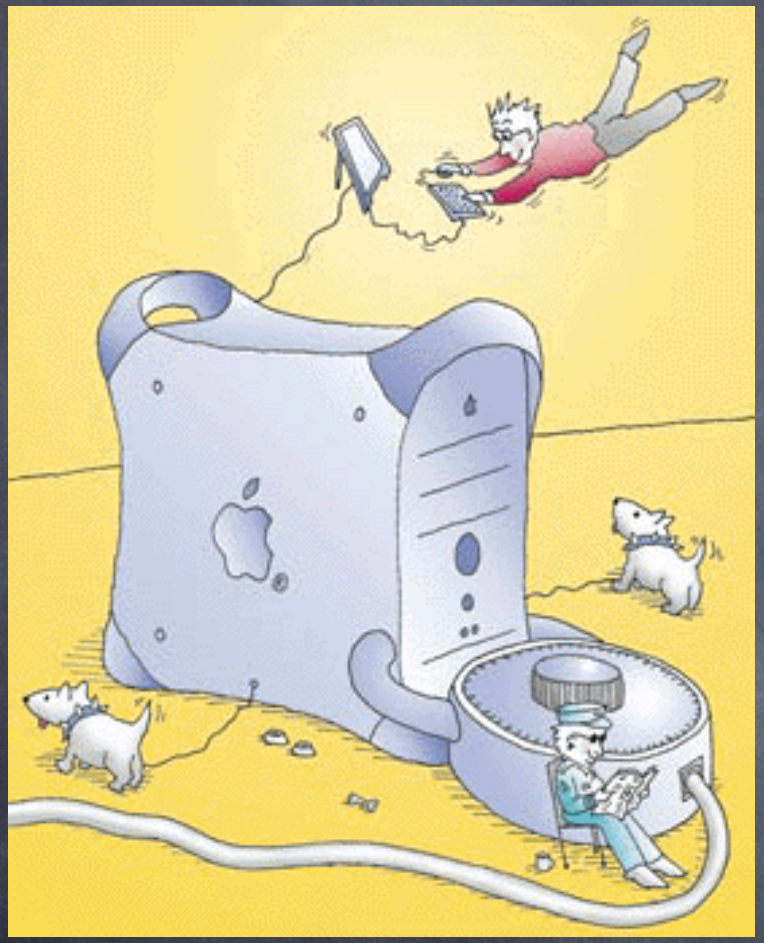


What EVERYONE Needs to Know About Internet Security

Alan Oppenheimer
January, 2006
Open Door Networks, Inc.

What everyone needs to know about this talk

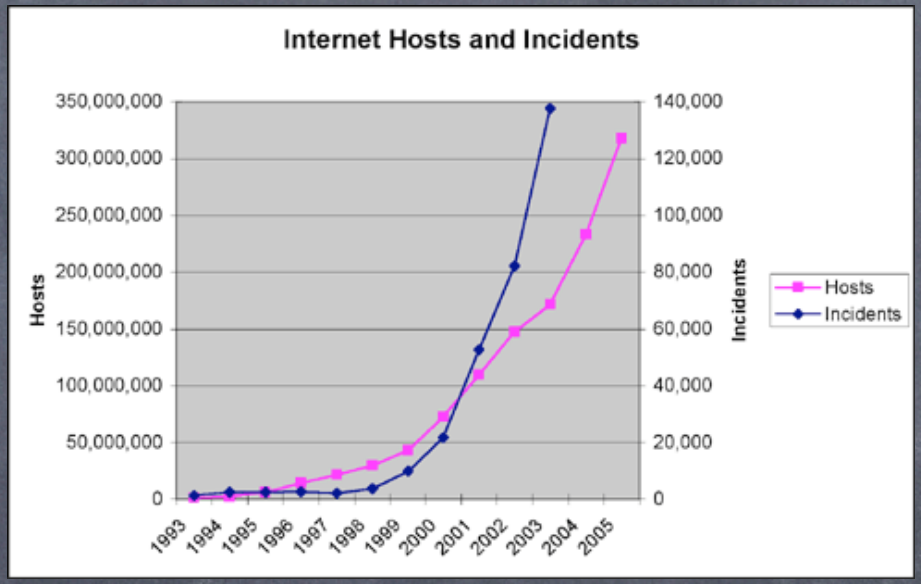
- Open Door Networks
- Alan B. Oppenheimer
- "Internet Security for You Macintosh: *A Guide for the Rest of Us*," 2nd edition
- The DoorStop X Security Suite

What, Me Worry?

- The Mac does have some security advantages
  - User-focus means better security design
  - Battlefield-hardened Unix code
  - Strength in (small) numbers
- But...

Yes, You Worry!

- More and more attacks



- The Net is more and more important
- Broadband connections particularly vulnerable

Why me?

- It's not about you!
- Hackers want to take over any machine(s) they can
- Then use those machines for evil deeds
  - Distributed denial of service attacks
  - Spam, phishing attacks, etc.
  - Implanting trojan horses

Physical Security

- More likely than an Internet attack:
  - Theft or loss (especially laptops)
  - Fire
  - Earthquake
  - Other "accident"
  - Hardware or software crash
  - Law enforcement seizure

So, lock the front door!

- Take appropriate physical security precautions
  - Secure building access
  - Pay particular attention to laptops
  - Lock-down cables, alarms, etc.
  - Surge protection and UPS

Backup, backup, backup

- Use backup applications or ad hoc methods
- Check backups
- Have local and remote backups
  - .Mac accounts
  - Apple's Backup Utility

Managing Passwords

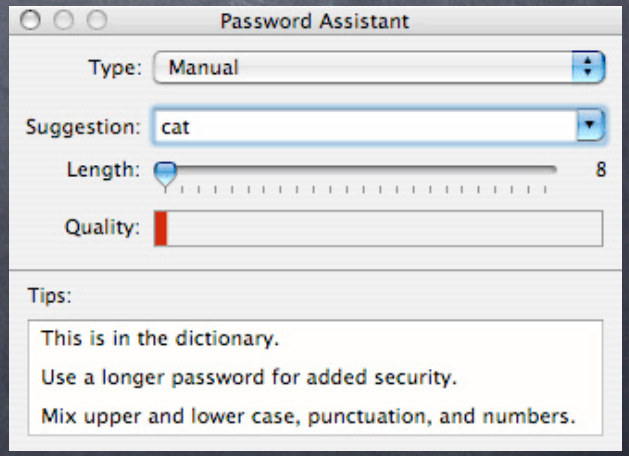
- More and more services need passwords
  - Email (often saved)
  - Web sites (sometimes important, often gratuitous)
  - Remote access (dial-in, PPPoE, VPN)
  - Your Mac's login/admin password

Properties of good passwords

- Should be very hard to guess
  - Longer is better
  - Numbers and special characters are better
  - Don't use real words (dictionary attacks)
  - No personal information
- Should be easy for you (and only you) to remember

Password management

- Keychain and other management apps
- Different passwords for different service levels
- Master passwords kept in a safe place
- Advanced solutions:
  - digital certificates
  - login once
  - biometrics



Keeping passwords secret

- Different passwords for different services
- Passwords changed periodically
  - But not often
- Don't make things too difficult for users
- Watch out for password compromise

Safe Surfing

- Secure Web
- Secure e-mail
- Secure IM and others

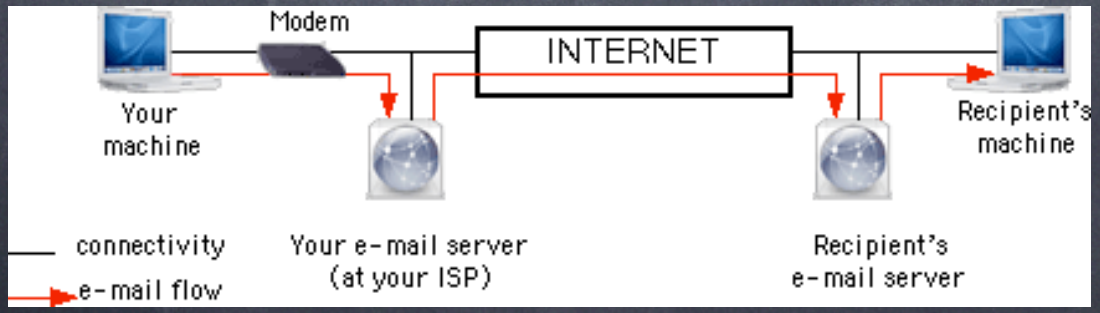
Safe Web

- Know if a site is secure or not
  - Encryption and authentication

- Secure sites safer than the "real world"
- Watch out for "phishing" though
- Way fewer worries than with Windows

Safe E-mail

- Attachments suck (but less on a Mac)
- Anyone can read your e-mail
- Anyone can send e-mail as you
- There are solutions...



Safe(r) e-mail solutions

- Password: APOP
- Encrypted e-mail: S/MIME,PGP,SSL
- Authenticated e-mail: S/MIME,PGP
- You still should avoid attachments though

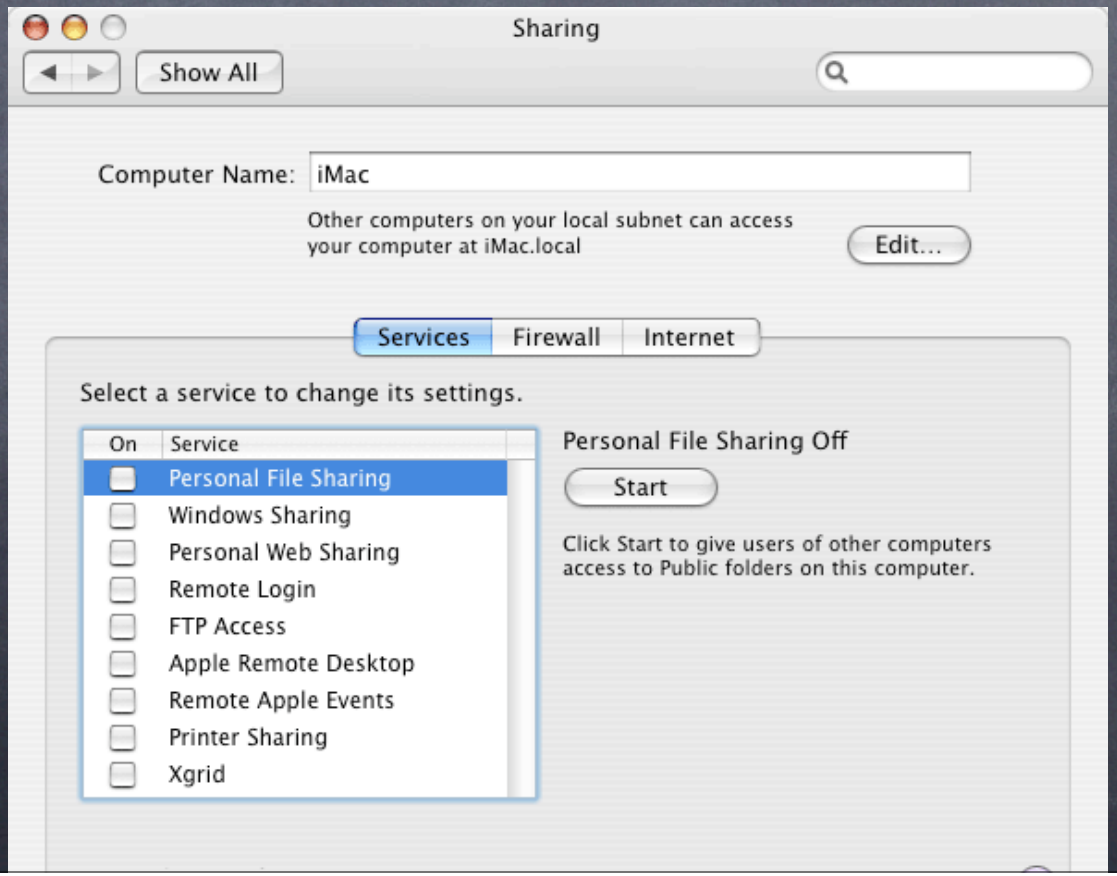
Phishing

- Fraudulent e-mail directing you to a fraudulent Web site
- E-mail and Web site look authentic
  - Somteimes very specifically crafted
- But they're just to steal your info
- Don't click on URLs in e-mail
- Call to be sure

Safe IM

- Anyone can read your IM (except new iChat)
- "On the Internet, no one knows you're a dog"
- Watch your kids especially closely
- Other new apps: peer-to-peer, VoIP

Using vs. providing services



Built-in Mac OS X services

- Personal File Sharing
- Windows Sharing
- Personal Web Sharing
- Remote Login
- Apple Remote Desktop

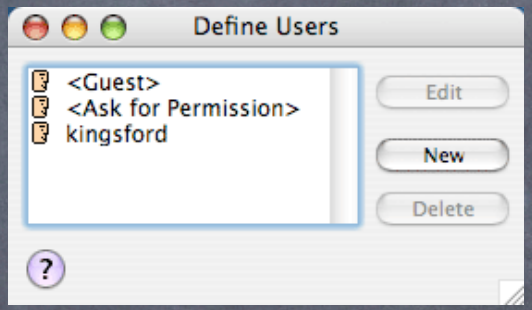
iApps

- iTunes Music Sharing
- iPhoto Photo Sharing
- iSync
- Disk Utility




Mac OS third-party services

- Timbuktu
- Retrospect
- FileMaker
- Virtual PC



Viruses

- Definition: hidden, self-executing, self-replicating, usually malicious programs
- Where they come from
  - More than just an Internet security issue
  - Net has let them spread more quickly and wider
- Probably the biggest Net security threat

Virus types

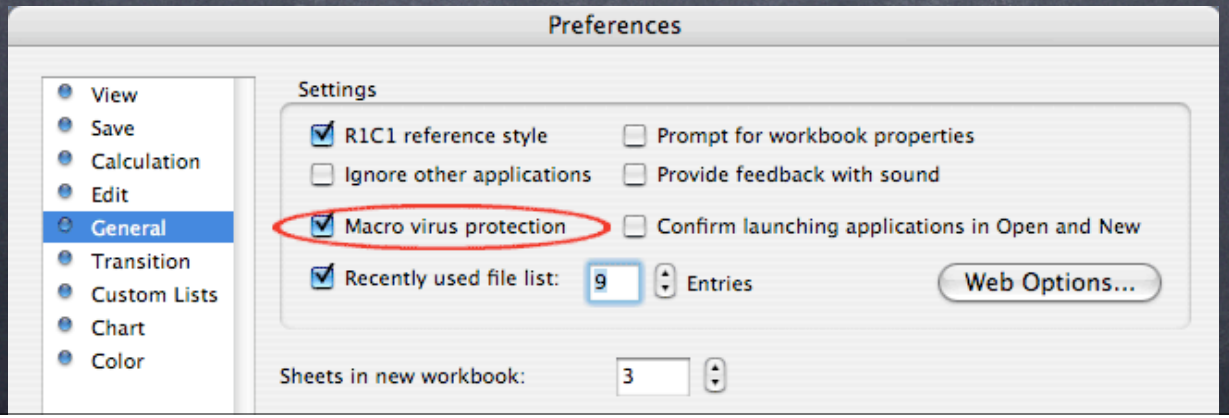
- OS virus vs. application virus
- Trojan horses - usually viruses
- Worms
- Macro/script viruses

What viruses can do

- Cause system crashes, corrupt files
- Steal passwords and other secrets
- Open your network to Internet attack
- Participate in distributed denial of service attacks
- Enable spam-sending, phishing

How to avoid viruses

- Macs are much less vulnerable
- Don't open attachments
- Minimize software downloading of any sort
- Disable macros



Anti-virus application

- What does it do?
  - Detects and block viruses, automatically
  - Removes viruses
- Purchase on CD
- Keep up on latest virus definitions

"Personal" firewalls

- Block unwanted access from the Internet or your intranet
- ...to specific services on the machine
- ...without interfering with normal network activities
- Log access attempts

Personal vs. network-global firewalls

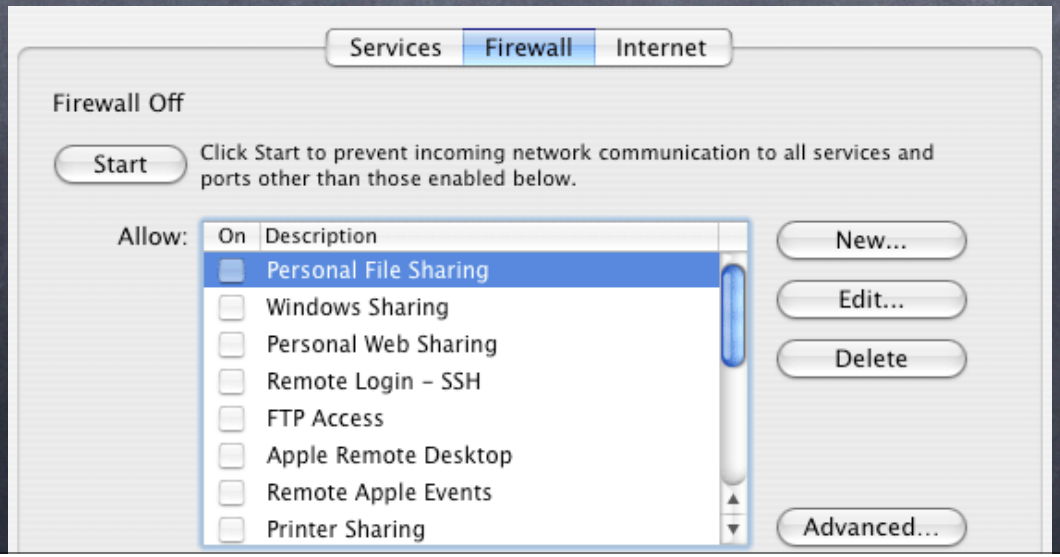
- "Personal" (machine-specific) protects the machine on which it's running
- Network-global protects a whole network, but doesn't protect against internal access
- Home networks should have both

Configuring your firewall

- Allow (deny) access to services (ports)
- Allow/deny access from IP addresses
- Defaults should always be the safest
- Log everything

Why you need more than Mac OS X's firewall

- Poor-to-non-existent logging
- All-or-nothing approach
- Limited UI



Analyzing and responding to security threats

- Analyze log information
  - Visually inspect log files (difficult, not real-time)
  - Analyze log files using analysis software
- Interpret the information
  - What does an access attempt mean?
- Respond if appropriate

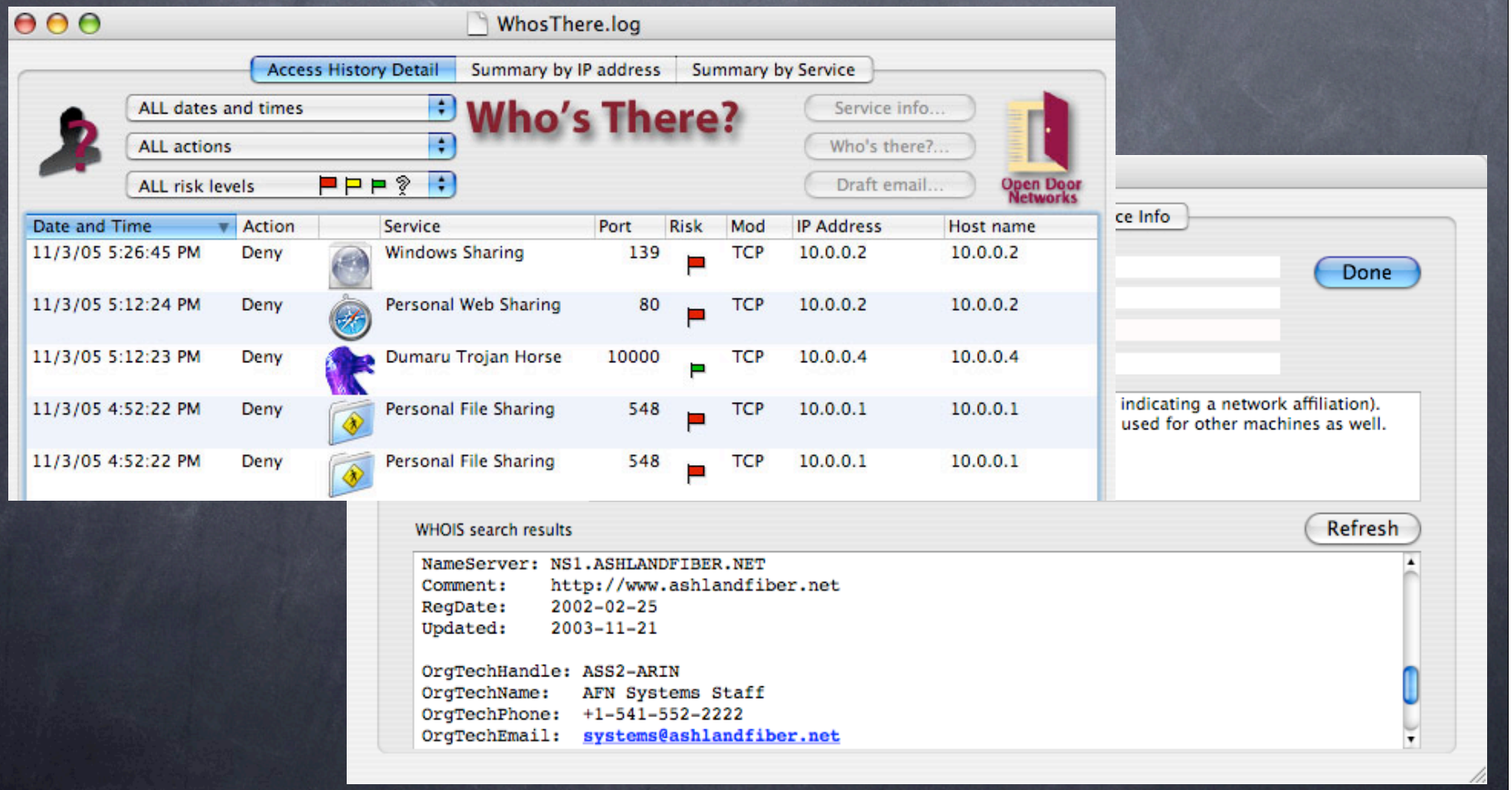
Responding to security threats

- Add layers of protection
  - Close open ports
  - Disable services if possible
  - Sure up passwords
- Locate and contact network administrators
  - Be polite
  - They're probably not responsible

Monitoring log files

- Need to do in real time
- Firewall log is key
- Automatically sift through lots of data
- Just look for key info
- Can react immediately to issues, prevent problems

Who's There?
Firewall Advisor



Key security issue : FTP

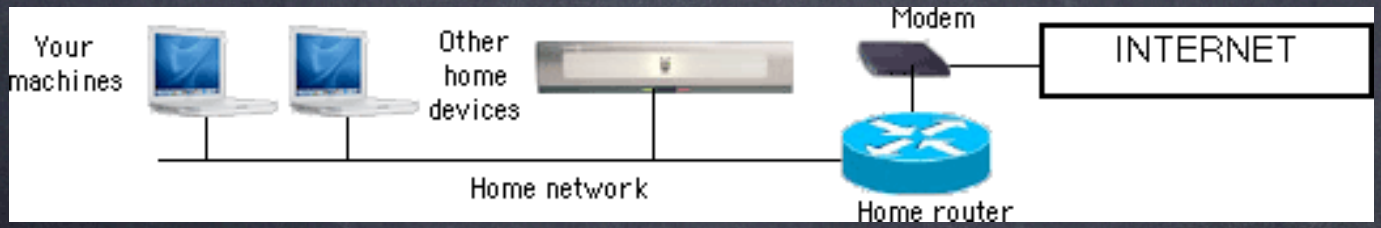
- A very old protocol
- Passwords sent in clear text!
- Does not work well with firewalls
- Harder for end users
- A very weak link in the security chain
- There are much better alternatives

FTP Alternatives

- AFP for Macs
- SMB for Windows
- HTTP SSL upload
  - Data secure too
- WebDAV
  - Cross-platform
  - Supported by Web page editors

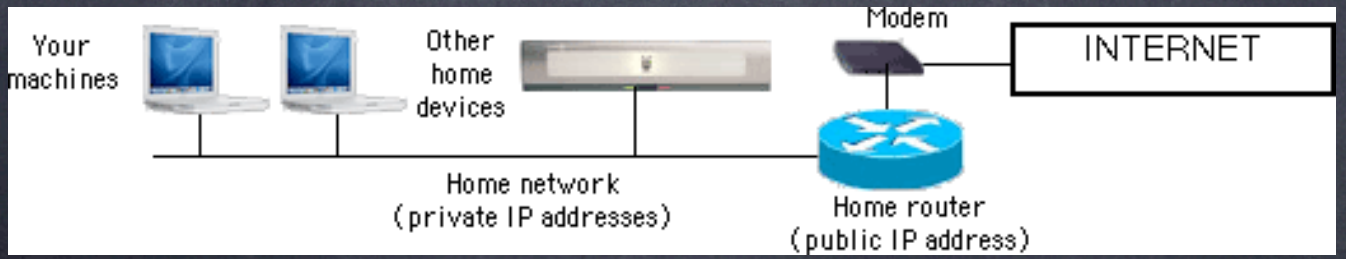
Home networks

- Mac-only and "mixed"
- Wired, wireless and mixed
- Share an Internet connection, files, or other home devices
- Almost always involve a home "router"



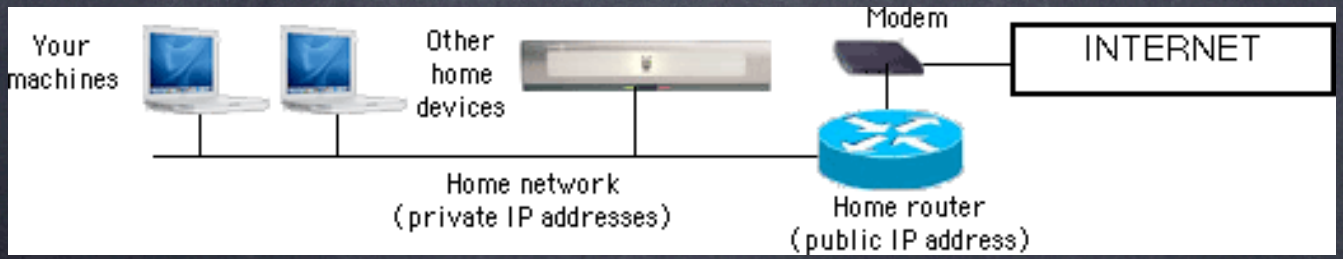
Home routers

- Interconnect devices within the home
- Connect home network to the Internet
- Share an Internet address (NAT)
- Act as a limited firewall
- Other new features (VPN...)



NAT

- Network Address Translation
- Multiple devices on the Net through one IP address
- Some firewall-like features
- Potential problems



Windows machines

- The weak link
  - More likely to be compromised, compromising whole network
  - Trojan horses can easily get "inside the firewall"
  - Cross-platform applications (Timbuktu)
  - Cross-platform viruses
  - Personal firewalls, anti-virus essential

Other home devices

- Digital media centers (TiVo)
- Phones
- Advanced devices

Wireless networking

- 802.11/AirPort
  - Built into many machines now
  - Computer-to-computer
  - AirPort base station
- Another weak link

Wireless security issues

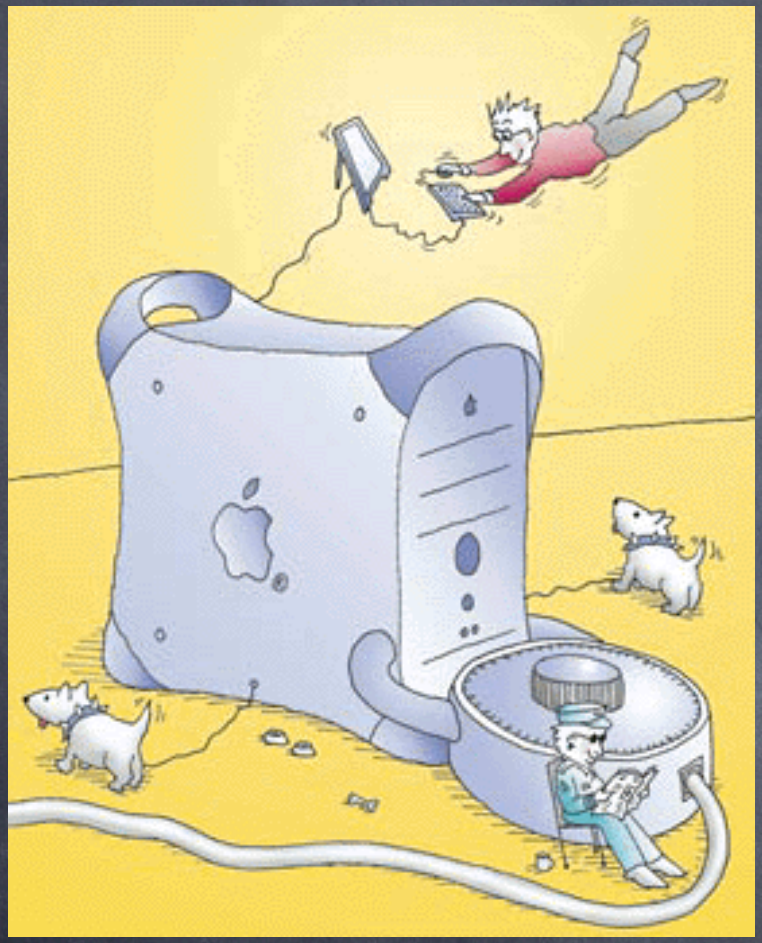
- Snooping
  - WEP (highly insecure)
  - WPA (much better)
- Unauthorized access
  - Network password
  - Closed networks
  - MAC ID limitations

Securing base station access

- Change base station password
- Restrict physical access to base station
- Only allow admin from local network
- Third-party base stations

Products

- "Internet Security for Your Macintosh: A Guide for the Rest of Us", 2nd edition
- DoorStop X Security Suite
  - DoorStop X Firewall
  - Who's There? Firewall Advisor
  - ISFYM



Q & A