#### Three case studies

- peer to peer networking
- wireless systems
- search engines
- each includes issues of
  - hardware

processors, storage, peripherals, networks, ... representation of information, analog vs. digital, bits & bytes

- software
  - applications, operating system, client-server and peer to peer organization of information, file systems, ...
    - algorithms: searching, sorting, compression
- communications, Internet, Web, TCP/IP, protocols bandwidth, speed, caching compression, error detection and correction
- security and privacy; cryptography
- intellectual property and ownership
- social & legal & policy concerns

### Peer to peer networking

- direct connections between peers
  - distributed instead of clients talking to single server
  - all clients provide bandwidth, storage, processing
- $\boldsymbol{\cdot}$  an old idea, though with a new name
  - USENET news service, 1979
- "peer-to-peer" file-sharing
  - centralized directories (original Napster in 1999)
  - decentralized directories (Gnutella, Kazaa, Limewire, Morpheus, etc.)
- once a file is found somewhere
  - set up direct connection between supplier and consumer ("peers")
  - applications use TCP/IP (same level as HTTP, SSH, SMTP, etc.)

#### other examples

- BitTorrent file distribution system
- Skype Internet telephony

## Peer to peer history

- Napster (1999-2001) [Shawn Fanning]
  - centralized real-time directory, distributed files
  - mostly MP3 music; ideal for Ethernet bandwidths
  - based in USA; lawsuits put it out of business
- Gnutella and friends (Grokster, Kazaa, ...)
  - decentralized directories: not as fast or reliable but less vulnerable to legal processes since no way to turn it off
- BitTorrent (2001)
  - distributed directories, distributed files
  - distributed peer servers for load-sharing: good for movies
- Digital Rights Management (DRM) systems
  - largely unsuccessful (awkward, inconvenient, don't really work anyway)
  - pay services like iTunes with reasonable DRM do better
- legal action
  - RIAA/MPAA lawsuit put Grokster out of business (2005)
  - numerous lawsuit threats against students and other individuals
  - Viacom sues Google over YouTube postings of movies & TV programs (2007)
- lobbying
  - numerous attempts to create more laws against file-sharing



## BitTorrent

- file-sharing for big files in high demand
- original file exists on at least one "seed" site
- "tracker" server knows who has what pieces
  - coordinates all transfers but does not have any of the file contents
- clients download blocks of file from multiple sources in parallel
  - blocks have cryptographic checksum to verify correct content
- $\cdot$  downloaded blocks also then uploaded to others
  - download rate limited by upload rate: have to contribute
  - tracker knows download and upload statuses balances traffic, favors sites that are cooperating
- blocks reassembled by client
  - when client has the whole file, it can be a seed for further transfers
- much faster than single server for right kind of use
  - less vulnerable to flash crowds
  - but takes time to get started, can't do streaming, etc.

## Internet telephony

- Voice over IP
  - package speech in IP packets
  - may connect to public telephone network on each end
  - strict requirements on delay (latency), jitter (variable delay), error handling, etc.
- lots of commercial providers (AT&T, Comcast, Verizon, Vonage,...)
  - alternative to conventional telephone service
  - somewhat cheaper, probably less reliable, maybe fewer services

#### • Skype: peer to peer VoIP

- comes from creators of Kazaa (!), claims no spyware or adware
- free within Internet, ~2 cents/min to connect to regular phone system
- 256-bit AES to encrypt each call, RSA to establish AES session key
- proprietary protocol, uses both TCP and UDP
- it can use your computer as a supernode (like Kazaa)
- Skype bought by eBay 10/05 for \$2.5B, sold again 11/09 for \$2B
- bought by Microsoft 10/11 for \$8.5B

# Technology meets law/policy/economics/politics

- should there be laws controlling peer to peer technology?
- should content providers like RIAA be permitted to install search (& destroy) software on home computers?
- should universities be required to enforce file-sharing laws?
- should VoIP be regulated by the FCC?
  - should VoIP suppliers have to provide services like 911?
  - should VoIP suppliers pay taxes and fees, and for connectivity to public telephone network?
  - should VoIP calls be subject to wire-tapping laws like regular phones?
- should common carriers like Verizon be permitted to discriminate against traffic from other VoIP suppliers?
  - should there be different prices and policies for different kinds of traffic?

### Net neutrality examples

- Comcast interferes with some BitTorrent traffic (2007)
  - claimed to be legitimate network management action to prevent a service from hogging bandwidth
  - when does a common carrier have the right to discriminate against some kinds of traffic to provide service to other kinds?
  - FCC told Comcast to stop; Comcast appealed;
  - 2010: court decided for Comcast because FCC lacks authority
- Verizon redirects failed DNS queries to its own search page instead of returning the failure status (2007)
  - example of DNS hijacking (for commercial purposes)
  - violates a standard protocol
  - breaks unrelated services (e.g., non-browser traffic)
  - overrides consumer choice of services
- what regulations, if any, should there be?
  - see http://itpolicy.princeton.edu/pub/neutrality.pdf

# Copyright issues

- digital media are intrinsically easy to copy
  - and hard to protect by technical means
- peer to peer enables copyright violation on a grand scale
- Digital Millennium Copyright Act (DMCA)
- test cases
- disclaimer
  - an enormous topic
  - IANAL

# Copyright

- protects expression, not idea
- duration used to be 17 years + one renewal
- now life + 70 years, or 95 years for commercial works
  - (the "Mickey Mouse Protection Act", 1998)
- "fair use" permits limited copying under some circumstances
  - criticism, comment, scholarship, research, news reporting, teaching
- uncertain what fair use really is -- case by case decisions
- considerations:
  - purpose and character of the use
  - nature of the copyrighted work
  - amount and substantiality of the portion used
  - effect of the use on potential market or value of copyrighted work
- recent copyright laws may prevent some fair uses
  - can't decrypt to make excerpt for teaching or criticism
  - can't reverse engineer to make copies in different media

## DMCA: Digital Millennium Copyright Act (1998)

- US copyright law: www.copyright.gov/title17, Chapter 12
- anticircumvention: illegal to circumvent a technological measure protecting access to or copying of a copyrighted work
  - limited exceptions for reverse engineering for interoperability, encryption research, security testing
- illegal to remove or alter copyright notices and management information
- "safe harbor": protects ISPs from copyright infringement claims if they follow notice and takedown procedures

### DMCA test cases

- Grokster
  - peer to peer software makes copyright infringement easy; are its distributors violating the DMCA?
- Diebold
  - internal emails reveal flaws in voting machine software; is posting of the emails a violation of DMCA?
- · SDMI
  - does demonstration of how to remove digital watermarking on audio files violate DMCA?
- Lexmark
  - cryptography used to prevent 3rd parties from supplying replacement ink cartridges; is reverse engineering a violation of DMCA?
- Viacom v Google
  - YouTube shows numerous copyrighted clips; is it sufficient that Google responds to individual takedown notices?
- · DeCSS
  - Content Scrambling System protects DVDs from copying; does publication of code to defeat it violate DMCA?

# DRM: Digital Rights (Restrictions?) Management

- techniques to control access to and use of digital material
- conflicts with fair use
  - prevents legitimate operations like time/space shifting, media conversion, backup, ...
  - a form of vendor lock-in?
  - obsolescent technology may cause things to be lost
- incompatible systems make users unhappy
  - may cause more trouble that it's worth
- pragmatically, DRM doesn't work and probably can't
  - Sony rootkit on audio CDs (2005): discovered immediately
  - iTunes FairPlay: cracked in 2006
  - Windows Media DRM: cracked in 2006-7
  - AACS (advanced access control system) encrypts HD-DVD and Blu-Ray: cracked in 2007
  - CSS (content scramble system) encrypts DVDs to prevent playing except on licensed players (and thus prevent copying): cracked in 1999
  - the analog hole as the last resort