312 Test review 2

Crime (ch. 5),

Work (ch. 6),

Evaluating and Controlling Technology (ch. 7),

Errors, Failures, and Risks (ch. 8),

Professional Ethics and Responsibilities (ch. 9)

What is Hacking?

- **Hacking** – currently defined as Intentional, unauthorized access to computer systems
- The term has changed over time
- Phase 1: early 1960s to 1970s
  - It was a positive term
  - A "hacker" was a creative programmer who wrote elegant or clever code
  - A "hack" was an especially clever piece of code

Hacking (cont.)

- Phase 2: 1970s to mid 1990s
  - Hacking took on negative connotations
  - Breaking into computers for which the hacker does not have authorized access
  - Still primarily individuals
  - Includes the spreading of computer worms, viruses and ‘phone phreaking’
  - Companies began using hackers to analyze and improve security

Hacking (cont.)

- Phase 3: starting the mid 1990s
  - The growth of the Web changed hacking; viruses and worms could be spread rapidly
  - Political hacking (Hacktivism) surfaced
  - Denial-of-service (DoS) attacks used to shut down Web sites
  - Large scale theft of personal and financial information

The Law re. Hacking

- 1984 Congress passed the Computer Fraud and Abuse Act (CFAA)
  - Covers government computers, financial and medical systems, activities that involve computers in more than one state, computers connected to the Internet
  - Outlaws hacking activities: DoS, malware, unauthorized access, fraud, impairing gov operations, public utilities
  - The USA Patriot Act expanded the definition of loss to include the cost of responding to an attack, assessing damage and restoring systems

Stealing Identities

- **Identity Theft** – various crimes in which a criminal or large group uses the identity of an unknowing, innocent person
  - Use credit/debit card numbers, personal information, and social security numbers
  - 18-29 year-olds are the most common victims because they use the web most and are unaware of risks
  - E-commerce has made it easier to steal card numbers and use without having the physical card

Theft Techniques

- Techniques used to steal personal and financial information
  - Phishing - e-mail fishing for personal and financial information disguised as legitimate business e-mail
    - Smishing – text messaging. Vishing – voice phishing
  - Pharming - planting false URLs in Domain Name Servers, lead to false Web sites that fish for personal and financial information
  - Online resumes and job hunting sites may reveal SSNs, work history, birth dates and other information that can be used in identity theft

Responses to Identity Theft

- Authentication of e-mail and Web sites
- Use of encryption to securely store data, so it is useless if stolen
- Authenticating customers to prevent use of stolen numbers, may trade convenience for security
- In the event information is stolen, a fraud alert can flag your credit report; some businesses will cover the cost of a credit report if your information has been stolen
- Biometrics: biological characteristics unique to an individual – "what you are"

Protection Techniques

- Preventing use of stolen numbers
  - Activation for new credit cards
  - Retailers do not print the full card number and expiration date on receipts
  - Software detects unusual spending activities and will prompt retailers to ask for identifying information
  - Services, like PayPal, act as third party allowing a customer to make a purchase without revealing their credit card information to a stranger

Libel law: threat to free speech

- Libel tourism: Traveling to places with strict libel laws in order to sue
  - SPEECH Act of 2010 makes foreign libel judgments unenforceable in the U.S. if they would violate the First Amendment. Foreign governments can still seize assets
- Where a trial is held is important not just for differences in the law, but also the costs associated with travel between the countries; cases can take some time to trial and may require numerous trips
- Freedom of speech suffers if businesses follow laws of the most restrictive countries

Cybercrime Treaty

- International agreement foster international cooperation among law enforcement agencies of different countries in fighting copyright violations, pornography, fraud, hacking and other online crime
- Treaty sets common standards or ways to resolve international cases
- It requires countries to outlaw some formally legal activities

“Responsibility to prevent access”

- So far governments are assuming a “Responsibility to prevent access” principle:

  It is the responsibility of providers of services and information to make sure their material is not accessible in countries where it is illegal. They may be sued or jailed in those countries if they do not prevent access

Alternative Principles

- So far governments are assuming a “Authority-to-prevent entry”:

  Government of Country A can act within Country A to try to block the entrance of material that is illegal there, but may not apply its laws to the people who create and publish the material, or provide a service, in Country B if it is legal there.

The Impact on Employment

Job destruction and creation:

- A successful technology eliminates or reduces some jobs but creates others
    - Reduced the need for telephone operators, electric meter readers, mid-level managers
- New industries arise
    - Chip industry, Internet, Cellular communications, clouds, smartphone software
- Lower prices increase demand and create jobs
    - Music industry changed from serving the wealthy to serving the masses, employing more than just musicians

A Global Workforce

- Outsourcing - a company pays another company to build parts for its products or services instead of performing those tasks itself
- Offshoring - the practice of moving business processes or services to another country, especially overseas, to reduce costs
- Inshoring - when another company employs thousands of people in the U.S. Almost 5% of U.S. workers work for foreign companies

Telecommuting Issues

Benefits

- Reduces employer overhead
- Reduces need for large offices
- Employees are more productive, satisfied, and loyal
- Reduces traffic congestion, pollution, gasoline use, and stress
- Reduces time and expenses for commuting and money spent on work clothes
- Allows work to continue after blizzards, hurricanes

Problems

- Employers see resentment from those who have to work at the office
- For some telecommuting employees, corporation loyalty weakens
- Odd work hours
- Cost for office space has shifted to the employee
- Security risks when work and personal activities reside on the same computer

Data Entry, Phone Work, Retail

- Data entry
  - Key stroke quotas
  - Public performance records to encourage competition
  - Beep when workers pause
- Phone work
  - Number and duration of calls
  - Idle time between calls
  - Randomly listen in on calls
- Retail
  - Surveillance to reduce theft by employees

Location Monitoring

- Cards and badges used as electronic keys increase security but track employee movements
- GPS tracks an employee's location
  - Used in some hospitals to track nurse locations for emergency purposes, but also shows where they are at lunch or when they use the bathroom
  - Used to track long-haul trucks to reduce theft and optimize delivery schedules, but also detects driving speeds and duration of rest breaks
- Employees often complain of loss of privacy

E-Mail, Blogging, and Web Use

- Some companies block specific sites (e.g. adult content, sports sites, job search sites, social-network sites)
- Employees spend time on non-work activities on the Web
- Concerns over security threats such as viruses and other malicious software
- Concerns about inappropriate activities by employees (e.g., harassment, unprofessional comment)

Evaluating Information

- Expert information or ‘wisdom of the crowd’?
  - Daunting amount of information on the web, much incorrect
  - Search engines are replacing librarians, but Web sites are ranked by popularity, not by expert evaluation
  - Search engines give prominent display to party who pay them
  - Wisdom of the crowd - ratings of website by public, democratic journalism for news

Narrowing the Information Stream

- The Web narrows information streams
- Some critics see the web as significantly encouraging narrowness and political extremes by making it easy for people to avoid seeing alternative opinions
- Searching online "puts researchers in touch with prevailing opinions, but this may accelerate consensus" and miss less popular but very relevant work
- People are seeing filtered information
  - Search engines, social media services personalize results based on location, past searches, profiles, etc.

Why Models May be Inaccurate

- Why models may not be accurate
  - We might not have complete knowledge of the system we are modeling
  - The data describing current conditions or characteristics may be incomplete or inaccurate
  - Computing power inadequate for the complexity of the model
  - It is difficult, if not impossible, to numerically quantify variables that represent human values and choices
- Ethical responsibility of professionals/modelers to honestly and accurately describe the results, assumptions, and limitations of their models

Neo-Luddite Views of Technology

- Computers eliminate jobs to reduce cost of production
- Computers manufacture needs; technology causes production of things we do not need
- Computers cause social inequity

Neo-Luddite Views of Technology

- Weaken communities, thwart development of social skills
- Computers separate humans from nature and destroy the environment
- Benefit big business and big government the most
- Do little or nothing to solve real problems

Failures and Errors in Computer Systems

- Most computer applications are so complex it is virtually impossible to produce programs with no errors
- The cause of failure is often more than one factor
  - Faulty design, sloppy implementation, careless users, poor user interface, insufficient user training…
- Design and testing of mission critical systems is much more complex than typical computer-based systems
- Computer professionals must study failures to learn how to avoid them, and to understand the impacts of poor work

System Failures

- AT&T, Galaxy IV satellite, Amtrak
- Businesses have gone bankrupt after spending huge amounts on computer systems that failed
- Voting systems in presidential elections
- Stalled airports: Denver, Hong Kong, Malaysia
- Abandoned systems
  - Systems discarded after wasting millions even billions of dollars
- Legacy systems
  - Reliable but inflexible, expensive to replace, little documentation

Denver Airport

- Baggage handling system costs ~ $200 million, caused most of the delay
- Baggage system failed due to real world problems, problems in other systems and software errors
  - Carts crashed into each other at track intersections, mistaken route. Scanner got dirty or knocked out of alignment, faulty latches, power surges
- Main causes:
  - Time allowed for development was insufficient
  - Denver made significant changes in specifications after the project began

High-level, management-related causes of computer-system failures

- Lack of clear, well thought out goals and specifications
- Poor management decisions and poor communication among customers, designers, programmers, etc.
- Institutional and political pressures that encourage unrealistically low bids, low budget requests, and underestimates of time requirements
- Use of very new technology, with unknown reliability and problems
- Refusal to recognize or admit a project is in trouble

Case Study: The Therac-25

Therac-25 Radiation Overdoses:

- Therac-25: a software controlled radiation therapy machine used to treat cancer patients
- 1985-1987, 4 medical centers
- Massive overdoses of radiation were given; the machine said no dose had been administered at all
- Caused severe and painful injuries and the death of three patients
- Important to study to avoid repeating errors
- Manufacturer, computer programmer, and hospitals/clinics all have some responsibility

Case Study: The Therac-25 (cont.)

Software and Design problems:

- Re-used software from older systems, unaware of bugs in previous software
- Weaknesses in design of operator interface
  - Obscure error messages with no documentation on them
- Inadequate test plan
- Bugs in software
  - Allowed beam to deploy when table not in proper position
  - Ignored changes and corrections operators made at console

What is "Professional Ethics"?

- Professional ethics includes relationships with and responsibilities toward customers, clients, coworkers, employees, employers, others who use one’s products and services, and others whom they affect
- A professional has a responsibility to act ethically
- Many professions have a code of ethics that professionals are expected to abide by
  - Medical doctors, Lawyers and judges, Accountants
- Honesty is one of the most fundamental ethical values; however, many ethical problems are more subtle than the choice of being honest or dishonest

Why Professional Ethics?

- Because of some special aspects
  - Professional is an expert in a field that most customers know little about
    - Customers have little ability to protect themselves, they rely on the knowledge, expertise, and honesty of the professional
    - This is regardless of whether they are the direct or indirect customers of the product
  - Products of many professionals (e.g., Highway bridges, investment advice, surgery protocols, computer systems) profoundly affect large number of people
  - Professionals must maintain up to date skills and knowledge

Professional Codes of Ethics

- Codes of two main computer professional orgs
  - ACM code of ethics and professional conduct

    ACM: Association of Computer Machinery
  - Software engineering (SE) code of ethics and professional practice

    IEEE-CS: Inst. for Electrical & Electronics Engineers, Computer Society

The SE Code (8 Principles)

1. Public: shall act consistently with the public interest
2. Client and employer: act in the best interest
3. Product: ensure to meet the highest standards possible
4. Judgment: maintain integrity and independence

The SE Code (8 Principles)

5. Management: ethical in management of software development and maintenance
6. Profession: advance the integrity and reputation
7. Colleagues: be fair to and supportive of their colleagues
8. Self: participate in lifelong learning in their profession

Total: 80 clauses

The ACM Code (24 Imperatives)

- General moral imperatives: as an ACM member, I will
  - Contribute to society and human well-being
  - Avoid harm to others
  - Be honest and trustworthy
  - Be fair and take action not to discriminate
  - Honor property rights including copyrights, patents
  - Give proper credit for IP (must not take credit for other’s idea or work)
  - Respect the privacy of others
  - Honor confidentiality

The ACM Code (cont’d)

- More specific professional responsibilities
  - Acquire and maintain professional competence,
  - Know and respect existing laws,
  - Honor contracts, agreements, and assigned responsibilities, …
- Organizational leadership imperatives
  - Articulate social responsibilities, encourage their full acceptance
  - Manage to design & build systems that enhance quality of life, …
- Compliance with the code
  - Uphold and promote the principles of this code, …

Conclusion

Conclusion for this course

- That is all!
  - I hope that this course has sparked a lot of ideas
  - I hope also that the discussion of risks and failures encourages you to exercise the highest degree of professional and personal responsibility
- Thank you!