Engineering Ethics

Lecture 7

Computer Ethics

- Computers are involved to some extent in almost every aspect of our lives
  - They often perform life-critical tasks
- Computer science is not regulated to the extent of medicine, air travel, or construction zoning
- Therefore, we need to carefully consider the issues of ethics

Computer Ethics

- Computer ethics are morally acceptable use of computers
  - i.e. using computers appropriately
- Standards or guidelines are important in this industry, because technology changes are outstripping the legal system's ability to keep up

Computer Ethics

- Computers have become the technological backbone of society.
- Computers raise a host of difficult moral issues, many of them connected with basic moral concerns such as free speech, privacy, respect for property, informed consent, and harm.
- The Internet has magnified all issues in computer ethics.
- Computers and the Internet dramatically increase the ability of centralized bureaucracies to manage enormous quantities of data.
- Computers are powerful tools that do not by themselves generate power shifts; they contribute to greater centralization or decentralization.

Computer Ethics

- Computer related issues
  - Job Elimination
  - Customer Relations.
  - Biased Software
  - Stock Trading
  - Military Weapons
- Crime by computer has proved to be unusually inviting; Computer crooks tend to be intelligent and to view their exploits as intellectual challenges.
- In addition, the computer terminal is both physically and psychologically far removed from face-to-face contact with the victims of the crimes perpetrated; unlike violent criminals, computer criminals find it easy to deceive themselves into thinking they are not really hurting anyone, especially if they see their actions as nothing more than pranks.

Computer Ethics

- There are often inadequate safeguards against computer crime.
- The technology for preventing crime and catching criminals has lagged behind the implementation of new computer applications.
- Computers reduce paperwork, but this has the drawback of removing the normal trail of written evidence involved in conventional white-collar crime (forgeries, receipts, etc.).
- Finally, the penalties for computer crime, as for white-collar crime in general, are mild compared with those for more conventional crimes.
- Computer crime raises obvious moral concerns of honesty, integrity, and trust.

Ethics for Computer Professionals

Computer Professionals:

- Are experts in their field,
- Know customers rely on their knowledge, expertise, and honesty,
- Understand their products (and related risks) affect many people,
- Follow good professional standards and practices,
- Maintain an expected level of competence and are up-to-date on current knowledge and technology, and
- Educate the non-computer professional

Computer Ethics

- Four primary issues
  - **Privacy** – responsibility to protect data about individuals
  - **Accuracy** - responsibility of data collectors to authenticate information and ensure its accuracy
  - **Property** - who owns information and software and how can they be sold and exchanged
  - **Access** - responsibility of data collectors to control access and determine what information a person has the right to obtain about others and how the information can be used

Data and Software

- Computer hardware is protected by **patent laws**.
- Software can be protected by **trade secret laws or by copyrights**.
- Trade secret laws permit employers to require their employees not to divulge proprietary information.
- Obviously, trade secrets are useless once software is made publicly available as a marketed product. Here copyright laws offer the best protection.
- Does a company steal the property of a software producer if it buys one copy and then reproduces dozens of copies for its other employees?
- Yes, unless a special agreement has been reached with the software producer.
- Is making a dozen copies of a program borrowed from a friend for resale stealing? Yes.

Problems with Large Databases

- Spreading information **without consent**
  - Some large companies use medical records and credit records as a factor in important personnel decisions

- Spreading **inaccurate** information
  - Mistakes in one computer file can easily migrate to others
  - Inaccurate data may linger for years

The Internet and the Web

- Most people don't worry about email privacy on the Web due to *illusion of anonymity*
  - Each e-mail you send results in at least 3 or 4 copies being stored on different computers.
- Web sites often load files on your computer called *cookies* to record times and pages visited and other personal information
- ***Spyware -*** software that tracks your online movements, mines the information stored on your computer, or uses your computer for some task you know nothing about.

General Internet Issues

- Inflammatory interchange of messages via internet (email, chat rooms, etc.)
- Chain mail
- Virus warning hoaxes
- “Spam” – unsolicited, bulk email

E-Mail Netiquette

- Promptly respond to messages.
- Delete messages after you read them if you don’t need to save the information.
- Don’t send messages you wouldn’t want others to read.
- Keep the message short and to the point.
- Don’t type in all capital letters.
- Be careful with sarcasm and humor in your message.

Internet Content & Free Speech Issues

- Information on internet includes hate, violence, and information that is harmful for children
  - How much of this should be regulated?
  - Do filters solve problems or create more?
- Is web site information used for course work and research **reliable**?

Information Ownership Issues

- Illegal software copying (pirating)
- Infringement of copyrights by copying of pictures or text from web pages
- Plagiarism by copying text from other sources when original work is expected

Privacy

- Storage, retrieval, and transmission of information using computers as data processors has revolutionized communication.
- Inappropriate Access or Hackings: suppose that the hacker's activities are limited to breaking into systems for shock value and a display of cunning. **Is that so bad?**
- All information ought to be freely available, that no one should be allowed to own information, especially in a democratic society that respects individual rights to pursue knowledge.
- Essentially, this argument makes freedom of information paramount.
- Yet, there are at least three other important values that place legitimate limits on access to information: individual privacy, national security, and freedom within a capitalist economy to protect proprietary information essential in pursuing corporate goals.

Terms

INTELLECTUAL PROPERTY: Intangible creations protected by law

TRADE SECRET: Intellectual work or products belonging to a business, not in public domain

COPYRIGHT: Statutory grant protecting intellectual property from copying by others for 28 years

PATENT: Legal document granting owner exclusive monopoly on an invention for 17 years

Copyright Laws

- Software developers (or the companies they work for) own their programs.
- Software buyers only own the right to use the software according to the license agreement.
- No copying, reselling, lending, renting, leasing, or distributing is legal without the software owner's permission.

Software Licenses

- There are four types of software licenses:
  - Public Domain
  - Freeware
  - Shareware
  - All Rights Reserved

Public Domain License

- Public domain software has no owner and is not protected by copyright law.
- It was either created with public funds, or the ownership was forfeited by the creator.
- Can be copied, sold, and/or modified
- Often is of poor quality/unreliable

Freeware License

- Freeware is copyrighted software that is licensed to be copied and distributed without charge.
- Freeware is free, but it’s still under the owner’s control.
- Examples:
  - Eudora Light
  - Netscape

Shareware License

- A shareware software license allows you to use the software for a trial period, but you must pay a registration fee to the owner for permanent use.
  - Some shareware trials expire on a certain date
  - Payment depends on the honor system
- Purchasing (the right to use) the software may also get you a version with more powerful features and published documentation.

All Rights Reserved License

- May be used by the purchaser according the exact details spelled out in the license agreement.
- You can’t legally use it--or even possess it--without the owner’s permission.

Software Piracy

- SPA (Software Publishers Association) polices software piracy and mainly targets:
  - Illegal duplication
  - Sale of copyrighted software
  - Companies that purchase single copies and load the software on multiple computers or networks
- They rely on whistle-blowers.
- Penalties (for primary user of PC) may include fines up to $250,000 and/or imprisonment up to 5 years in jail

Computer Crime

- Computer criminals -using a computer to commit an illegal act
- Who are computer criminals?
  - Employees – disgruntled or dishonest --the largest category
  - Outside users - customers or suppliers
  - “Hackers” and “crackers” - hackers do it “for fun” but crackers have malicious intent
  - Organized crime - tracking illegal enterprises, forgery, counterfeiting

Types of Computer Crime

- Damage to computers, programs or files
  - Viruses - migrate through systems attached to files and programs
  - Worms - continuously self-replicate
- Theft
  - Of hardware, software, data, computer time
  - Software piracy - unauthorized copies of copyrighted material
- View/Manipulation
  - “Unauthorized entry” and “harmless message” still illegal

Computer Security

- Computer security involves protecting:
  - information, hardware and software
  - from unauthorized use and damage and
  - from sabotage and natural disasters

Measures to Protect Computer Security

- Restricting access both to the hardware locations (physical access) and into the system itself (over the network) using firewalls
- Implementing a plan to prevent break-ins
- Changing passwords frequently
- Making backup copies
- Using anti-virus software
- Encrypting data to frustrate interception
- Anticipating disasters (disaster recovery plan)
- Hiring trustworthy employees

Ten Commandments of Computer Ethics

1. Thou shalt not use a computer to harm other people.
2. Thou shalt not interfere with other people's computer work.
3. Thou shalt not snoop around in other people's computer files.
4. Thou shalt not use a computer to steal.
5. Thou shalt not use a computer to bear false witness.
6. Thou shalt not copy or use proprietary software for which you have not paid (without permission).
7. Thou shalt not use other people's computer resources without authorization or proper compensation.
8. Thou shalt not appropriate other people's intellectual output.
9. Thou shalt think about the social consequences of the program you are writing or the system you are designing.
10. Thou shalt always use a computer in ways that ensure consideration and respect for your fellow humans.[

Created in 1992 by the Computer Ethics Institute.

References

1. Introduction to Engineering Ethics (Basic Engineering Series and Tools) 2nd Edition
2. Computer Ethics, Privacy and Security, Lecture Slide from Regis University, Colorado, USA
3. http://computerethicsinstitute.org/publications/tencommandments.html