Computer Ethics, Privacy and Security

Computer Ethics

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

Ethics

- Ethics are standards of moral conduct
  - Standards of right and wrong behavior
  - A gauge of personal integrity
  - The basis of trust and cooperation in relationships with others

Ethical Principals

- Ethical principals are tools which are used to think through difficult situations.
- Three useful ethical principals:
  - An act is ethical if all of society benefits from the act.
  - An act is ethical if people are treated as an end and not as a means to an end.
  - An act is ethical if it is fair to all parties involved.

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

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

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

Private Networks

- Employers may legally monitor electronic mail
  - In 2001, 63% of companies monitored employee Internet connections including about two-thirds of the 60 billion electronic messages sent by 40 million e-mail users.
- Most online services reserve the right to censor content
- These rights lead to contentious issues over property rights versus free speech and privacy

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

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

System Quality

- Bug-free software is difficult to produce
- It must be carefully designed, developed, and tested
- Mistakes generated by computers can be far reaching
- Commenting and documenting software is required for effective maintenance throughout the life of the program

System Quality

ETHICAL ISSUES:

When is software, system or service ready for release?

SOCIAL ISSUES:

Can people trust quality of software, systems, services, data?

POLITICAL ISSUES:

Should government or industry develop standards for software, hardware, data quality?

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

Computer Ethics for Computer Professionals

- **Competence**– Professionals keep up with the latest knowledge in their field and perform services only in their area of competence.
- **Responsibility**– Professionals are loyal to their clients or employees, and they won't disclose confidential information.
- **Integrity**– Professionals express their opinions based on facts, and they are impartial in their judgments.

The ACM Code of Conduct

- According to the Association for Computing Machinery (ACM) code, a computing professional:
  - **Contributes to society and human well-being**
  - **Avoids harm to others**
  - **Is honest and trustworthy**
  - **Is fair and takes action not to discriminate**
  - **Honors property rights, including copyrights and patents**
  - **Gives proper credit when using the intellectual property of others**
  - **Respects other individuals' rights to privacy**
  - **Honors confidentiality**

Joint IEEE-CS/ACM Code of Ethics and Professional Practice

- Built on 8 principles
  - Public Interest
  - Client and Employer
  - Product
  - Judgement
  - Management
  - Profession
  - Colleagues
  - Self
- The principle of Public Interest is central to the code.

Public Interest

- Software engineers shall act consistently with the public interest.
  - Approve software only if they have a well-founded belief that it is safe, meets standards, passes tests and does not diminsh quality of life, privacy or harm the environment.
  - Disclose any actual or potential danger to the user.
  - Be fair an davoid deception in all statements concerning software.

Client and Employer

- Software engineers shall act in a manner that is in the best interests of their client and employer, consistent with the public interest.
  - Be honest about any limitation of their experience and education.
  - Keep private any confidential information consistent with the public interest and the law.
  - Not knowingly use software that is obtained or retained either illegally or unethically.

Product

- Software engineers shall ensure that their products and related modifications meet the highest professional standards possible.
  - Strive for high quality, acceptable cost, and a reasonable schedule, ensuring significant tradeoffs are clear.
  - Ensure adequate testing, debugging, and review of software and related documents on which they work.
  - Treat all forms of software maintenance with the same professionalism as new development.

Judgement

- Software engineers shall maintain integrity and independence in their professional judgment.
  - Not engage in deceptive financial practices.
  - Disclose to all concerned parties those conflicts of interest that cannot reasonably be avoided or escaped.

Management

- Software engineering managers and leaders shall subscribe to and promote an ethical approach to the management of software development and maintenance.
  - Ensure that software engineers are informed of standards before being held to them.
  - Offer fair and just remuneration.
  - Not punish anyone for expressing ethical concerns about a project.

Profession

- Software engineers shall advance the integrity and reputation of the profession consistent with the public interest.
  - Promote public knowledge of software engineering.
  - Be accurate in stating the characteristics of software on which they work.
  - Take responsibility for detecting, correcting, and reporting errors in software and associated documents on which they work.

Colleagues

- Software engineers shall be fair to and supportive of their colleagues.
  - Credit fully the work of others and refrain from taking undue credit.
  - Give a fair hearing to the opinions, concerns, or complaints of a colleague.
  - In situations outside of their own areas of competence, call upon the opinions of other professionals who have competence in that area.

Self

- Software engineers shall participate in lifelong learning regarding the practice of their profession and shall promote an ethical approach to the practice of the profession.
  - Further their knowledge
  - Improve their ability to create safe, reliable, and useful quality software
  - Improve their ability to produce accurate, informative, and well-written documentation.

Problems with codes of conduct

- They don’t cover every case (nor should they).
- Can a list of rules define a behaviour that everyone considers right?
- Little penalty for non-compliance
  - Requires a Personal Code of Ethics that is broadly in line with the Professional Code.

Ethical Delemma 1: Reverse Engineering

- When is reverse engineering ethical?
- Scenario: You are asked to produce software to read in a file (with an undisclosed proprietary format) into an application.
  - Test vectors and analysis?
  - Decompilation?
    - "Clean room" environment

Ethical Delemma 2: Whistle Blowing

- If you believe that knowledge of unethical practices would cause a change in the practices:
  - Reality check (make sure you are right)
  - The goal is to get management to recognise and remedy problem with minimal conflict.
  - Take problem outside the organisation as last resort and act as an individual, not an employee.
- Be prepared to live with the results.
- Document everything.
- Be on your best behaviour.