Computer Engineering Ethics
CMP1102

Course details

- 2 mid-terms (40%)
- Final Exam (60%)
- References

[1] Kenneth E. Himma, Herman T. Tavani, 2008. The Handbook of Information and Computer Ethics. Wiley-Interscience. ISBN-10: 0471799599 , ISBN-13: 978- 0471799597

[2] J. Fernando Naveda and Stephen B. Seidman, 2006. *IEEE Computer Society Real- World Software Engineering Problems: A Self-Study Guide for Today's Software Professional (Practitioners).* Wiley-IEEE Computer Society Pr. ISBN-10: 0471710512 , ISBN-13: 978-0471710516

[3] Winn Schwartau, D. L. Busch, 2001. *Internet & Computer Ethics for Kids: (and Parents & Teachers Who Haven't Got a Clue.)*. Interpact Press. ISBN-10: 0962870056, ISBN-13: 978-0962870057

What is Ethics?

- Each society forms a **set of rules** that establishes the boundaries of generally accepted behavior.
- These rules are often expressed in statements about how people should behave, and they fit together to form the **moral code** by which a society lives.
- **Ethics** is the study of the moral choices made by each person in his/her relationships with other people.
- Ethical behavior conforms to generally accepted social norms, many of which are almost universal.
- **Virtues** are habits that incline people to do what is acceptable, and **vices** are habits of unacceptable behavior
- People's virtues and vices help define their **value system** – the complex scheme of moral values by which they live

Engineering Ethics

What is engineering ethics?

(1) The rules and standards which govern the conduct of engineers in their role as professionals

(2) The study of moral issues and decisions confronting individuals and organizations involved in engineering.

What are the purposes for Code of Ethics for Engineers?

- Provide positive stimulus for ethical conduct
- Helpful advice concerning the primary obligation of "engineers"
- Guideposts in interpreting ethical dilemmas

Code of Ethics that Apply to Computer Engineers?

- IEEE Code of Ethics
- IEEE-CS/ACM Software Engineering Code of Ethics and Professional Practice
- National Society of Professional Engineers Code of Ethics

Preamble NSPE Code of Ethics

- Engineering is an important and learned profession.
- Engineers are expected to exhibit the highest standards of honesty and integrity.
- The services provided by engineers require honesty, fairness and equity, and must be dedicated to the protection of the public health, safety, and welfare.
- Engineers must perform under a standard of professional behavior that requires adherence to the highest principles of ethical conduct

What are Professional Ethics?

- Professional ethics are a code of conduct that govern how members of a profession deal with each other and with third parties.

Why should we have a Professional Code of Ethics? (1/2)

- A Professional Code of Ethics serves several functions:
  - Symbolises the professionalism of the group.
  - Defines and promotes a standard for external relations with clients and employers.
  - Protects the group's interests.
  - Codifies members' rights.
  - Expresses ideals to aspire to.
  - Offers guidelines in "gray areas".

Why have a Professional Code of Ethics in Computing? (2/2)

- Software has the potential to do good or cause harm, or to enable or influence others to do good or cause harm.
- We have pride in our work and want the work that we do to be given recognition and respect.
- We want to protect our livelihood.

Some Examples

- ACM Code of Ethics and Professional Conduct.
  - http://www.acm.org/constitution/code.html
- IEEE-CS/ACM Software Engineering Code of Ethics and Professional Practice
  - http://www.computer.org/tab/seprof/code.htm

Characteristics of a Code of Ethics

- They are not simple ethical algorithms that generate ethical decisions.
- Sometimes elements of the code may be in tension with each other or other sources.
  - Requires the software engineer to use ethical judgement to act in the spirit of the code of ethics.
- A good code of ethics will enunicate fundemental principles that require thought rather than blind allegience.

Quote on Ethics

Quote from Aristotle:

“Man, when perfected, is the best of the animals, but when separated from law and justice, he is the worst of all”

Why Study Ethics

- Increased awareness of importance due to publicity surrounding high profile engineering failures
- Engineering decisions can impact public health, safety, business practices and politics
- Engineers should be aware of moral implications as they make decisions in the workplace.
- Study of ethics helps engineers develop a moral autonomy:
  - Ability to think critically and independently about moral issues
  - Ability to apply this moral thinking to situations that arise in the course of professional engineering practice
- Ethical problems in engineering are often complex and involve conflicting ethical principles. Engineers must be able to intelligently resolve these conflicts and reach a defensible decision

Common Ethical Issues for IT Users (1/2)

- **Software Piracy**: a common violation occurs when employees copy software from their work computers for use at home
- **Inappropriate Use of Computing Resources**: some employees use their work computers to surf popular Web sites that have nothing to do with their jobs.

  "Half of Fortune 500 companies have dealt with at least one incident related to computer porn in the workplace over the past 12 months, according to a survey released today.
  Corporations are taking the problem seriously, and fired the offenders in 44% of the cases and disciplined those responsible in 41% of the instances".

  (China Martens, Survey: Computer porn remains issue at U.S. companies, Computer-world, June 21, 2005

Common Ethical Issues for IT Users (2/2)

- **Inappropriate Sharing of Information:**
  - Organizations stored vast amount of information that can be classified as private or confidential.
  - Private data describes individual employees – for example, salary, attendance, performance rating, health record.
  - Confidential information describes a company and its operations: sales, promotion plans, research and development.
  - Sharing this information with unauthorized party, even inadvertently, has violated someone's privacy or created the potential that company information could fall into the hands of competitors.

Supporting The Ethical Practices of IT Users (1/3)

- **Defining and Limiting the Appropriate Use of IT Resources**
  - Companies must develop, communicate and enforce written guidelines that encourage employees to respect corporate IT resources and use them to enhance their job performance.
  - Effective guidelines allow some level of personal use while prohibiting employees from visiting objectionable Web sites or using company e-mail to send offensive or harassing messages.

Supporting The Ethical Practices of IT Users (2/3)

- **Establishing Guidelines for Use of Company Software**
  - Company IT managers must provide clear rules that govern the use of home computers and associated software.
  - The goal should be to ensure that employees have legal copies of all software
- **Structuring Information Systems to Protect Data and Information**
  - Implement system and procedures that limit data access to employees who need it.
  - Employees should be prohibited from accessing the data about research and development results, product formulae, and staffing projections if they don't need it

Supporting The Ethical Practices of IT Users (3/3)

- **Installing and Maintaining a Corporate Firewall**
  - Firewall is a software or hardware device that serves as a barrier between a company and the outside world and limits access to the company's network based on the Internet usage policy.
  - Firewall can be configured to serve as an effective detergent unauthorized Web surfing by blocking access to specific, objectionable Web sites.
  - Firewall can serve as an effective barrier to incoming e-mail from certain Web sites, companies or users
  - Can be programmed to block e-mail with certain kinds of attachments, which reduces the risk of harmful computer viruses

Computer and Internet Crime
IT Security Incidents

- The security of IT used in business is very important
- Although, the necessity of security is obvious, it often must be balanced against other business needs and issues
- IT professionals and IT users all face a number of ethical decisions regarding IT security:

Ethical Decisions Regarding IT Security (1/2)

- Business managers, IP professionals, and IT users all face a number of ethical decisions regarding IT security:
  - If their firm is a victim of a computer crime, should they pursue prosecution of the criminals at all costs, should they maintain a low profile to avoid the negative publicity, must they inform their affected customers, or should they take some other actions?
  - How much effort and money should be spent to safeguard against computer crime (how safe is safe enough?)

Ethical Decisions Regarding IT Security (2/2)

- If their firm produces software with defects that allow hackers to attack customer data and computers, what actions should they take?
- What tactics should management ask employees to use to gather competitive intelligence without doing anything illegal?
- What should be done if recommended computer security safeguards make life more difficult for customers and employees, resulting in lost sales and increasing costs?

What could be done to deal with the increasing number of IT-related security incidents, not only in USA but around the world?

- To deal with the incidents, the Computer Emergency Response Team Coordination Center (CERT/CC) was established in 1988 at the Software Engineering Institute (SEI) – federally funded research and development center at Carnegie Mellon:
  - Study Internet Security vulnerabilities
  - Handle Computer Security Incidents
  - Publish Security Alerts
  - Research long-term changes in networked systems
  - Develop information and training
  - Conduct ongoing public awareness campaign

Some Statistics

- The number of security problems reported to CERT/CC grew between 1997 and 2003 from 2134 to 137,529
- From 2004 the CERT/CC no longer publishes the number of incidents reported

Challenges (1/4)

- Increasing complexity increases vulnerability:
  - The computing environment has become very complex
  - Networks, computers, OS, applications, Web sites, switches, routers and gateways are interconnected and driven by hundreds of millions of lines of code
  - The number of possible entry points to a network expands continually as more devices are added, increasing the possibility of security breaches

Challenges (2/4)

- Higher computer user expectations:
  - Time means money
  - Help desks are under intense pressure to provide fast responses to user's questions.
  - Sometimes forgets to verify user's identities, or to check authorization to perform a requested action

Challenges (3/4)

- Expanding and changing systems introduce new risks:
  - Businesses had moved from an era of stand-alone computers to a network era – personal computers connect to networks with millions of other computers all capable of sharing information.
  - E-commerce, mobile computing, collaborative work groups, global business
  - It is increasingly difficult to keep up with the pace of technological change, successfully perform an ongoing assessment of new security risks, and implement approaches for dealing with them

Challenges (4/4)

- Increases reliance on commercial software with known vulnerabilities:
  - **Exploit** is an attack on an information system that takes advantage of a particular system vulnerability. Often, this attack is due to poor system design or implementation.
  - Once a vulnerability is discovered, software developers create and issue a “fix” or **patch** to eliminate the problem. Users are responsible for obtaining and installing the patch. Any delay in installing a patch exposes the user to a security breach.
  - A rate of discovering software vulnerabilities exceeds 10 per day, creating a serious work overload for developers who are responsible for security fixes.

Challenges: Increases reliance on commercial software with known vulnerabilities (1/2)

- **A zero-day** attack take place BEFORE the security community or a software developer knows about a vulnerability or has been able to repair it.

  http://www.computerworld.com/securitytopics/security/hacking/story/0,10801,90447,00.html?f=x583

- Malicious hackers are getting better and faster at exploiting flaws.
- The SQL Slammer worm appeared in January 2004, eight month after the vulnerability it targeted was disclosed:

  http://www.computerworld.com/softwaretopics/software/groupware/story/0,10801,89637,00.html

Challenges: Increases reliance on commercial software with known vulnerabilities (2/2)

- In August 2005, the ZOTOB computer worm began targeting corporate networks that run Windows 2000, less than a week after Microsoft released a critical patch addressing the vulnerability

  http://www.cnn.com/2005/TECH/internet/08/16/computer.worm/index.html

- In an attempt to avoid further attacks and the ultimate zero-day attack, computer security firms and software manufactures are paying hackers to identify vulnerabilities before they can be exploited.

  http://www.businessweek.com/magazine/content/05_34/b3948022_mz011.htm?chan=tc

Types of Attacks

- Security incidents can take many forms, but one of the most frequent is an attack on a networked computer from outside source.
- Most attacks involve:
  - Viruses
  - Worms
  - Trojan Horses
  - Denial – of – Service (DoS)

Viruses (1/3)

- ***Computer virus*** has become an umbrella term for many types of malicious code.
- Technically, ***virus*** is a piece of programming code that seeks out other programs and “infects” a file by embedding a copy of itself inside the program. The infected program is often called a virus host. When the host procedure runs, the virus code runs as well and performs the instruction it was intended to perform. [1]
- A ***virus*** needs a ***host*** to infect. Without a host, the virus cannot replicate.

Viruses (2/3)

- **Viruses** cause some unexpected and usually undesirable event.
- Most **viruses** deliver a “payload” or malicious act. For example, the virus may be programmed to display a certain message on the screen, delete or modify certain document, or reformat the hard drive.
- A true **virus** doesn’t spread itself from computer to computer. To propagate to other machines, it must be passed through e-mail attachment, shared files, etc…. It takes action by the computer user to spread a virus.
- **Macro virus**: attackers use an application macro language (Visual Basics Scripting) to create programs that infects documents and templates. After an infected document is opened, the virus is executed and infects the user’s application template. Macros can insert unwanted words, numbers or phrases into documents. After a macro virus infects user’s application, it can embed itself in all future documents created with the application

Viruses (3/3)

- Virus is a program that can be broken into three functional parts [2]:
  - Replication
  - Concealment
  - Bomb

Worms

- A ***worm*** is different from a virus in that it is a standalone program [1].
- A typical ***worm*** maintains only a functional copy of itself in active memory and duplicate itself [2]. They differ from viruses because they can propagate without human intervention, sending copies of themselves to other computers by e-mail, for example.
- In the last few years, the boundary between worms and viruses has become increasingly blurry, starting with ***Melissa*** (1999).
- ***Melissa was a worm/virus hybrid*** that could infect a system like a virus by modifying documents to include quotes from *The Simpsons* TV show. But it could also use the Address Book in Microsoft Outlook and Outlook Express to resend itself like a worm to other clients, who where then subsequently infected by an attached document (which might be a confidential document [2]).

Trojan Horse (1/2)

- The ***Trojan horse*** is an application that hides a nasty surprise [2].
- The ***Trojan horse*** is a program that a hacker secretly installs on a computer.
- The program harmful payload can allow the hacker to steal password, SSN, or spy on users recording keystrokes and transmitting them to a server operated by a third party. The data may then be sold to criminals who use this info to obtain credit cards.

Trojan Horse (2/2)

- The ***Trojan horse*** is standalone application that appears to perform some helpful or neutral purpose, but is actually performing a malicious act while the user watches the program appear to do something else [1], [2].

- ***Trojan horse*** doesn’t replicate itself, and doesn’t attach itself to other files.

Logic Bomb

- Type of Trojan horse, which executes under specific conditions.
- A logic bomb can execute based on a date and time, or when you shut down your machine for the 33rd time [1] or based on typing a specific series of keystrokes. Any event works.

References

[1] Information Security Illuminated, Michael G. Solomon, Mike Chapple, Jones and Bartlett Publishers, Inc.

[2] Mastering Network Security, Chris Brenron, Cameron Hunt, Sybex Inc.