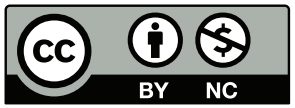
Ethics II



Ethics and Computer Science

- Last class, we discussed some historical scenarios
- We'll now consider some issues as they apply to computer science
- We'll look at project-specific issues and those that demand professional skill
- We'll consider ethical considerations towards both the public at large and towards our employer

Project Goals

- Is it good for the country or world if this system should exist?
- What about likely spinoffs or follow-ons?
- If you weren't paid to do it, would you want to live in the resulting world?

Example: Ballistic Missile Defense

- It seems obvious that it would be nice to be able to shoot down incoming nuclear missiles
- However, one can argue that the existence of such a technology makes a nuclear war *more* likely

MAD

- For about 60 years, we've avoided nuclear war through "MAD" — Mutually Assured Destruction
- Both the U.S. and the U.S.S.R. had enough capability to absorb a devastating first strike and still destroy the other country
- ABM systems change the equation

MAD vs. ABM

- Any ABM system is imperfect — some percentage of missiles *will* get through
- If a first strike knocks out a lot of one side's missiles, the counterstrike will be smaller
- This in turn means that the ABM system will be more effective; the counterstrike may not destroy enough to deter whomever launched the first strike
- This creates an incentive for a massive surprise attack. . .
- (Of course, U.S. missile subs are largely invulnerable to preemptive strikes, which complicates matters even more.)

A Multilateral World

- MAD was a strategy for a two-party world: the U.S. (plus NATO, though that's a complication I won't go into) versus the U.S.S.R. (China had little or no ICBM capability.)
- Many more potentially hostile powers have nuclear bombs and missiles now
- Is a limited ABM system — one too small to destabilize the balance with Russia — now more rational?

Issues

- Given the strategic balance, is it good or bad for the world for an ABM system to exist?
- (This issue is one reason, among several, why the U.S. and the U.S.S.R. signed a treaty in 1972 drastically limiting ABM systems.)
- What about a limited ABM system, aimed at smaller states, accidental launches, or the *Dr. Strangelove* scenario?
- Is defense more moral than offense, and especially more moral than MAD?
- Who gets to decide? What is the ethical obligation for computer scientists?

Example: Deep Packet Inspection

- Some ISPs are deploying “Deep Packet Inspection” technology.
- Some countries are deploying “Deep Packet Inspection” technology.
- Is this good or bad?
- (What is Deep Packet Inspection?)

Deep Packet Inspection

- Ordinary firewalls work on packet headers: IP addresses and port numbers.
- (A *port number* is more or less an identifier for a specific service on a computer. The web is on port 80, mail is received on port 25, etc.)
- *Deep Packet Inspection* (DPI) is technology that permits examination of the *payload* of packets: what the actual message is.
- A DPI-based firewall could perhaps block web traffic that appeared to be hostile, such as the Internet Explorer that is rumored to have been used against Google
- Older firewalls could only block known-evil destinations

DPI and Firewalls

- DPI poses few ethical issues for corporate firewalls
- In general, corporations own their networks and the machines behind them, and insist on the right to monitor all activity
- This grants no new rights; it just makes certain monitoring easier
- But — is it reasonable for corporations to have that power?

DPI and ISPs

- Some ISPs are deploying DPI to look at customer traffic
- Detect and block P2P traffic (the RIAA and the MPAA want this)
- Monitor consumer behavior, to improve targeted advertising
- Modify consumer web traffic, to insert ads
- (More on this topic when we discuss privacy)

Is that Proper?

- Is there a privacy issue?
- Does this violate consumer expectations for Internet service?
- Should the free market settle this? (Is there an effective market for broadband consumer Internet?)

DPI and Countries

- "The Iranian regime has developed. . . one of the world's most sophisticated mechanisms for controlling and censoring the Internet. . . " (all quotes from WSJ, 6/22/09)
- "China's vaunted 'Great Firewall' . . . is believed also to involve deep packet inspection."
- "Britain has a list of blocked sites, and the German government is considering similar measures. In the U.S., the National Security Agency has such capability"
- "The Australian government is experimenting with Web-site filtering to protect its youth from online pornography"
- "Internet censoring in Iran was developed with the initial justification of blocking online pornography"

Rationale

- “Mr. Roome of Nokia Siemens Networks said the company ‘does have a choice about whether to do business in any country. We believe providing people, wherever they are, with the ability to communicate is preferable to leaving them without the choice to be heard.’”
- “Nokia Siemens Networks provided equipment to Iran last year under the internationally recognized concept of ‘lawful intercept’”
- “Content inspection and filtering technology are already common among corporations, schools and other institutions, as part of efforts to block spam and viruses, as well as to ensure that employees and students comply with computer-use guidelines. Families use filtering on their home computers to protect their children from undesirable sites, such as pornography and gambling.”

Is Working on DPI Ethical?

- It has many very legitimate uses
- It's also a technology that can be and has been misused
- Who is responsible for making the ethical decision? Programmers? Corporate executives who sell the product? Users of it?
- What is the right answer?

ABM Systems Redux: Can We Build One?

- An ABM system requires a massive amount of software
- You can never really test the system, since its behavior will depend on the precise timing of the precise inputs — radar signals, number of incoming missiles, enemy decoys, how many computing nodes have already been knocked out or are misbehaving because of radiation, etc.
- The 1970s and 1980s ABM systems required nuclear-armed missiles — all controlled by this large, complex, untestable software system. . .
- What is the ethical response?

Professional Ethics

- Different professions have specific ethical principles
- Example (AMA): “An individual’s opinion on capital punishment is the personal moral decision of the individual. A physician, as a member of a profession dedicated to preserving life when there is hope of doing so, should not be a participant in a legally authorized execution.”
- Example (ABA): “As a representative of clients, a lawyer performs various functions. . . As advocate, a lawyer zealously asserts the client’s position under the rules of the adversary system. . . A lawyer’s representation of a client, including representation by appointment, does not constitute an endorsement of the client’s political, economic, social or moral views or activities.”
- The computing profession has several codes of ethics, too

The ACM Code of Ethics

- (The Association for Computing Machinery is the oldest professional organization in the field, founded in 1947.)
- “As an ACM member I will. . . Contribute to society and human well-being.”
- “Avoid harm to others. ‘Harm’ means injury or negative consequences, such as undesirable loss of information. . . ”
- “Respect the privacy of others. . . This imperative implies that only the necessary amount of personal information be collected”
- “Give comprehensive and thorough evaluations of computer systems and their impacts, including analysis of possible risks.”

ACM Software Engineering Code of Ethics

- “Moderate the interests of the software engineer, the employer, the client and the users with the public good.”
- “Approve software only if they have a well-founded belief that it is safe, meets specifications, passes appropriate tests, and does not diminish quality of life, diminish privacy or harm the environment. The ultimate effect of the work should be to the public good.”
- “Disclose to appropriate persons or authorities any actual or potential danger to the user, the public, or the environment, that they reasonably believe to be associated with software or related documents.”
- “Identify, document, collect evidence and report to the client or the employer promptly if, in their opinion, a project is likely to fail, to prove too expensive, to violate intellectual property law, or otherwise to be problematic.”

What Do These Excerpts Say?

- First: you have a responsibility to society
- Second: that you must conduct your professional life in accordance with this principle
- In particular, you have to *honestly* assess a system design, especially if there are risks to others

Special Roles Have Special Concerns

- (SAGE/Usenix/LOPSA Code of Ethics) “I will access private information on computer systems only when it is necessary in the course of my technical duties. I will maintain and protect the confidentiality of any information to which I may have access, regardless of the method by which I came into knowledge of it.”
- On most computers, a system administrator can override any protection mechanisms.
- Often, it is *necessary* to do so to keep things running smoothly

Other Possible Issues

- A project will fail because it is too complex, or with too little time or money
- A system design is likely to prove unreliable

☞ This can be very hard to prove, especially because it's often a subjective judgment based on experience

- A system poses privacy risks

☞ In some countries, that can be a matter of law, too

What to Do?

- Go to your management?
- Go public? What about confidentiality agreements?
- Inform legal authorities?
- Resign? (In this economy?)

To What Extent are These Principles Honored?

- We've all seen and used awful computer systems
- What is the proper balance between cost and {function, reliability, security, privacy, etc.}?
- Who draws that line?
- What is the responsibility of the individual?