CS 523: Social, Economic, and Legal Aspects of Security

Cyber Ethics
Morality

• Every culture or group has guidelines to regulate the behavior of its members
  – Guidelines = set of shared rules, principles, duties
  – Purpose of guidelines is to create happiness for (and harmony among) the group’s members

• Such groups define morality as conformity to the group’s guidelines
  – They judge acts as right or wrong, good or bad, based on their conformity to group’s guidelines
Morality (cont’d)

• Moral guidelines depend on location, culture
  – Can also change over time
• They have commonality across location and time
• Carl Sagan’s universal moral code
  – Be friendly at first meeting
  – Do not envy
  – Be generous; forgive the enemy who forgives you
  – Be neither a tyrant nor a patsy
  – Retaliate proportionately to intentional injury (if legal)
  – Make your behavior fairly clear and consistent
Ethical theories

• Aim to justify moral guidelines to outsiders
• Why bother with outsiders? Isn’t it enough to have social justification (“all insiders agree”)?
• Because there is need for rationality and rigor
  – Results are required to have some plausibility, a lack of logical contradictions (unlike social)
• Rationality and rigor can clash with social
  – Socrates, Galileo, Voltaire
Codes of ethics

• Can take various forms
  – Principles, policies, codes of conduct
  – Legal instruments (enforceable by courts)

• Can have many objectives
  – Disciplinary
  – Good publicity for members
  – Advisory/educational
  – Inspirational
Codes of ethics (cont’d)

• Codes of ethics
  – Domain-specific (for us, the cyber domain)
  – Especially needed when technical decisions involve ethical tradeoffs (as in cyber domain)

• Role of professional societies (ACM, IEEE)
  – http://www.acm.org/about-acm/acm-code-of-ethics-and-professional-conduct
  – http://www.ieee.org/about/corporate/governance/p7-8.html
When in doubt about an action

• Imagine the roles are reversed
  – How would you feel if someone did this to you?
• Imagine it reported in tomorrow’s newspaper
  – How would you feel it it were on the front page?
• Imagine your parents (or a respected mentor)
  – Would they go ahead and do it? What would they think of your doing it?
• How did similar past actions by others fare?
Ethical theories: Consequentialism

- Judging an act based on its consequences
- Does not concern itself with whether an act’s perpetrator had a good reason to do it or not
- Extreme form: Actions towards achieving a morally important goal are acceptable
  – “The end justifies the means”
Ethical theories: Deontological

• Centers on the act itself, not its consequences
  – E.g., good acts can have bad consequences
• Judges an act based on its own merits
• Often rule-based
  – An act is judged based on whether it conforms to rules (or duties, obligations)
  – The perpetrators of the act are judged based on whether they complied or not
Ethical theories: Pragmatism

• Societal progress through a process of inquiry
  – Similar to the way science progresses
  – Focus on society, not the individual

• Holds that none of the current moral criteria is immune from potential future revision
  – Even criteria that are strongly held today
  – Just like currently believed scientific theories can be replaced with better theories in the future (the truth can differ from current beliefs about it)
Ethical dilemmas

- When none of the available choices available is unambiguously good or acceptable
  - Obeying one moral imperative leads to the transgression of another
- Example: “Do not lie” v.s. causing harm
  - Physical harm to the truth-teller, or to others (the “Nazi at your door” situation)
- Example: Stealing food v.s. letting family die
- Lesser evil view, greater good view
Ethical dilemmas (cont’d)

• Issues with quantitative (“lesser”, “greater”)
  – Trolley
  – Transplant
  – Violent rioters
  – Sophie’s choice
  – Lifeboat
  – Blocked cave entrance

• Others
  – Good Samaritan, moral hazard
Examples for discussion

• Example 1: Alice violated her employer’s cyber-policy, but the violation ended up being beneficial to her employer
  – Thwarted a break-in, increased profits

• Example 2: Cyber-thieves break into a system, use the info in it to expose a serious cover-up
  – Cover-up had negative societal consequences

• Roles of malice and forethought
Disclosure of software vulnerabilities

• Dealing with vulnerabilities
  – Vulnerabilities can be eliminated through a software patch released by software vendor
  – Or their effects neutralized by measures taken by the organizations where the software is deployed
  – Either case requires the vulnerabilities to have been disclosed to the vendor and potential victims

• Which disclosure procedures give advantage to defense and disadvantage to attackers?
Non-Public Disclosure

• Disclose only to a few agencies known to behave responsibly (like CERT or similar)
• These agencies immediately notify software vendors, so they can start working on a patch
  – These agencies publicly disclose only after the security patch is available from the software vendor (usually 1 to 6 months after vendor was notified)
• Widely considered the responsible alternative
Non-Public Disclosure (cont’d)

• Advantages
  – Does not prematurely inform attackers of vulnerability
  – Gives vendors a head start over attackers

• Drawbacks
  – Potential victims can remain unaware of the vulnerability for months
  – Pointless to wait when attackers may have discovered the vulnerability on their own
Immediate Public Disclosure

• Publicly disclose as soon as vulnerabilities are discovered
  – Use mailing lists (e.g., BugTraq)

• Disadvantage
  – Potential attackers can use the information to their advantage before a patch is available

• Advantages
  – Can force unresponsive software vendors to more promptly develop a patch
Immediate Public Disclosure (cont’d)

• Advantages (cont’d)
  – Security personnel of potential victims are more alert than if they did not know – they can promptly work on countermeasures, and may develop effective ones before a patch is available
  – Incentivizes software vendors to develop secure software

• Evidence in favor of “more public” disclosures
  – i.e., disclose to more than just software vendor