COMPUTER ETHICS EDUCATION: IMPACT FROM SOCIETAL NORMS

Gregory B. White
Udo W. Pooch, Ph.D.

Texas A&M University

ABSTRACT

Discussions have occurred on the best way to implement the horizontal and vertical integration of education on the social, ethical and professional issues relating to computer science. These discussions have not only included debates on the subject matter and what manner to approach it (i.e. integrated among all computer science courses taught, as a separate required course, or a combination of both), but have also involved debates over who is best qualified to address the subject. What has seldom been addressed, however, is how societal impressions of what is ethical have impacted both those who develop software and those who use it. In light of the experience of such institutions as the U.S. Air Force Academy which recently instituted a program called the Center for Character Development (due to a perceived erosion of the core values of its recruits), should academia and industry expect more from computer scientists than from the population as a whole? It is the integration of ethics courses in the computer science curriculum in light of a general erosion of ethical values in society as a whole that is addressed in this paper.

BACKGROUND

Stories of computer 'hacking', viruses, and 'phone phreaking' have become all too common today. Incidents such as the group of hackers from the former West Germany who broke into numerous computers in this country, and who then sold information they obtained and details of what they did to foreign intelligence services has moved hacking from the pages of fiction writers to front page headlines. Anybody who uses computers has heard about the damage that can be caused by viruses. Incidents such as the Internet Worm created by Robert Morris has insured this type of malicious software has also received its share of headlines. Even more ominous to some are the exploits of individuals such as Kevin Mitnick who exploited not only computer systems and networks but was adept at manipulating telephone service as well [4]. As new legislation has moved such incidents from being mere nuisances to criminal offenses, society needs to insure that the proper and ethical usage of the new electronic frontier is taught to all who choose to use it. Unfortunately, the blossoming of this new frontier is occurring at a time in this country when societal standards have changed and have produced a new generation whose basic moral values have also changed. Nowhere has this been more apparent than at the United States military service academies.

Each year, more than a thousand of the top high school students in the country are admitted to each of the military service academies. For years these institutions have been known for their strict code of honor and their adherence to such ideals as Duty, Honor, and Country. Recently, however, the new recruits arriving at the academies have exhibited a lack of what was once considered common ethical values. According to Lt. Col. Terrence Moore, ethics director at the United States Air Force Academy, the cadets seem to lack "things like integrity and selflessness, responsibility, decisiveness, honesty -- basic core values" [9]. This apparent change in basic values is so pronounced that it prompted officials at the Air Force Academy to create the Center for Character Development. The purpose of this new organization is to help instill character into the new cadets [9]. Assuming that this change in ethical norms found at the Academy is not confined to this institution but is indicative of society as a whole, should it be a surprise that abuses of 'proper networking protocol' [7] occur? If our high school graduates exhibit surprise that ethnic and racial slurs may offend some [1] should we expect the newest generation of network users to act differently? It appears that if a certain standard of ethical conduct is to be expected, it must be taught to those expected to live by it. What then

Ethics in Computer Age, Gatlinburg,TN USA
© 1994 ACM 0-89791-644-1/94/0011...$3.50

is it that needs to be taught and how best is this to be accomplished?

ETHICAL ISSUES THAT SHOULD BE ADDRESSED

Appropriate conduct in some areas of ethical behavior is easier to teach than others. Many aspects of computer crime, for example, are easier for most people to grasp. Abuses of automated teller machines (ATMs) and electronic funds transfer (EFT) systems is becoming more common but is obvious to all as criminal activity. Other areas such as software piracy and new laws governing 'hacking' and malicious software, however, are often hard to understand. To many individuals involved with breaking into computer systems and networks, their activities seem like harmless intrusions that have not caused any damage. What harm, after all, occurred if they simply looked at a few files or read some email messages? The issue of an individual's right to privacy is often harder to understand when the victim is a faceless entity. Just like a small child who has to be taught that it is not polite to enter someone's room and start looking through their possessions, users of computer networks need to be taught that snooping through someone's files and email is also not polite or ethical.

The image of the 'hacker' presented in this country has also made it more difficult for those who are concerned with promoting ethics and responsibility in computing. For too long the public's perception of the normal computer intruder was a high school (or younger) student who was doing it for fun, not for any malicious intent. Movies such as *War Games*, released a decade ago, served to further glorify the image of the hacker. In this movie, the hero, a young high school student, accidentally breaks into an important government computer while searching for a new video game. By the end of the movie, in which he is responsible for almost starting World War III, the hero has actually done a service for the country by exposing the possible harm this government computer could do. His activities are not promoted as illegal or unethical, even when trying to obtain an unauthorized copy of the video game. Instead we are presented with the image of an intelligent young student, who only wanted to play games, pitted against the evil government computer system and those who run it. Even in a more recent movie, *Sneakers*, many of these same images are still being presented to the public. In this movie the age of the intruders has increased (they now start hacking in college) but we still are presented with the premise that it is the government that is performing unethical activities, not our heroes who only happen to stumble across the evil government program. One positive aspect of *Sneakers* , however, was that it showed that a criminal element could use the same techniques employed by the heroes to perform illegal activity. Newspapers do no better in presenting the true picture of hackers in this country. *Bloom County*, a popular cartoon, featured a number of hacker and computer piracy cartoons in which young Oliver Wendell Jones pillaged corporate and government computer systems. Once again the public was presented with the same, non-offensive, image of computer hackers and software pirates.

The ethical issues surrounding software piracy has long been a difficult challenge to address. Estimates from the U.S.-based Software Publishers' Association put losses due to software piracy at between $10 and $12 billion dollars a year [2]. The very term 'software piracy' lessens the perceived severity of the action as it conjures up images of the swashbuckling hero seen in many films produced by Hollywood. Pirates were thieves and software piracy is nothing more than software theft. A related but even more difficult issue to understand is that of intellectual property rights. Adding to the confusion surrounding this somewhat nebulous topic are several court cases addressing the 'look and feel' issue of software packages. Lotus' success in their suits relating to their popular 1-2-3 package seem to contradict the failures Apple has met with in their suits relating to 'Macintosh-style' interfaces. Add to this the often confusing rulings on software patents and copyrights and the result is an environment that is not likely to soon be settled [2,3].

Part of the problem with the copyright, intellectual property rights, and patent issues is the mixed signal that is often sent to software developers. The Internet was developed with the idea of a free exchange of ideas. Practically any type of software desired is available for free via anonymous FTP. Whenever a useful tool or program is developed, many similar programs will soon be found on the net. Parodies of popular packages are also commonly found. Is it any surprise then, that Delrina Corporation released a parody of the popular Berkeley Systems' After Dark screen-saver in 1993? This parody, called Opus N' Bill, had the popular cartoon character Opus shooting at a series of flying toasters. Unfortunately for Delrina, a judge ruled against them when Berkeley Systems sued for copyright and trademark infringement [6].

In another area, however, the issues are easier to understand. As a result of such cases as the Internet Worm and the Friday the 13th Virus, the public has become somewhat familiar with the potential effects of malicious software. The damage caused by these programs and the fear that they instill in users serves to make this another area in which the ethical issue is understood. Developing software that causes damage, while possibly a challenge to write, is not considered a proper thing to do.

An area in which the ethical responsibility of programmers is not clearly understood is in the effect of unreliable software. What are the implications of software that doesn't work? Who, if anyone, should be held responsible when software that is critical fails? Who is to blame if software, which is being used by a system which is needed to sustain human life, quits working? What about a financial program whose failure results in the bankruptcy of a business? What is a reasonable level of testing for software? An even more interesting dilemma is the one presented to software developers who may become aware of unethical, illegal, or immoral conduct of their employers. What is the responsibility of a programmer who discovers the program under development is to be used by individuals to commit some form of 'white collar' crime? Does the programmer have some moral or ethical obligation in this case? These are just a few of the many facets to the ethics question which must be addressed in an organized fashion if we are to ever hope to establish a core computer ethics value system.

TEACHING COMPUTER ETHICS

The 1991 ACM report on Computing Curricula recommended both a vertical and horizontal integration of Social, Ethical and Professional issues into the new curriculum. Realizing, however, that the largest number of new users has not come from the technical side but rather from business, humanities, and the social sciences, it is obvious that more is needed than just a new core computer science course. Whenever a new user is given access to a network or computer system they should be trained on what is considered appropriate conduct. Just like a child must be instructed on what is considered appropriate, these 'network and computer children' must be told what they should and should not do. Additionally, just like the child is corrected (and possibly punished depending on the severity of the offense), individuals who abuse their privileges should also be corrected and punished should the incident warrant it.

Those who develop software need additional instruction in accordance with their increased level of responsibility. This additional instruction should not simply take the form of a single course on computer ethics but rather should be incorporated as an integral aspect of all courses. This does not mean that every computer science course must spend several hours discussing ethical and societal issues but rather computer science departments should make it understood that they consider that there is an ethical standard that they expect all students to live up to. There are certain courses where mention of the standards should be made. The first required course in the curriculum should spend a couple of hours discussing specific elements of the standard (such as 'hacking', malicious software, and privacy issues). In another course, such as a software engineering or a programming language course, the ACM Code of Ethics should be used as a guide to further discuss ethical issues as they apply to computer science. In other courses which may have specific societal or ethical impact issues, a lesson should be spent addressing them. Even with periodic mention of ethics and societal issues, a separate course on this subject should be offered for those who want to further explore them.

A related issue is the message that is sent to students when abuse is tolerated. Sometimes "hackers" are looked upon as "guru's" whose abilities are to be revered. Abuses of ethics and privacy cannot, however, be tolerated and the most important message a university's computer science department can send is that they will not accept or tolerate such activity.

SUMMARY

There has been a change in the core ethical values in this country which can be seen in its high school graduates. With this change, it is unrealistic to expect users of computer systems to behave in a manner which they may not realize is considered inappropriate or unethical. Just like raising a child to function ethically in society requires a certain amount of training, we must provide training to raise users of computer systems and networks to be responsible members of this new electronic society. This will require a 'grass roots' effort to train new users before they are given access to and are allowed to function in this electronic society. Just like an individual must demonstrate an understanding of the rules of the road before they can receive a driver's license, computer and network users should be required to demonstrate an understanding of the rules of the 'electronic highway' before they are allowed to travel on it (and, if they violate any of these rules, they should be held accountable as are users of our asphalt highways).

Beyond this introduction, however, additional instruction needs to be provided to those who are allowed increased access and privileges. For programmers who will be developing the vehicles that are to be used on the electronic highway, additional instruction should be provided to ensure that this increased access is used properly. Even more important than this, however, is the need for computer science departments, and the industry in general, to establish a standard and to adhere to it so that all know that the 'electronic' or 'digital highway' is one area where ethical behavior is not only encouraged but expected and enforced.

In addition, we need to stop glorifying the exploits of the abusers of this electronic frontier. We need to use appropriate terms, such as software theft, instead of adding an air of legitimacy to actions by using terms such as 'piracy'. We cannot allow the abusers of this frontier to be turned into some new type of frontier hero as individuals such as Jesse James or Billy the Kid were for the frontier of the old west. These new electronic bandits should be recognized as outlaws and handled accordingly.

Finally, we, as computer professionals, should continue the dialogue frequently seen in such publications as the Communications of the ACM and the IEEE Computer Society's Computer magazine on issues relating to ethics [8]. It is only through discussions like these that any standard will eventually be realized.

REFERENCES

1. Anton, Genevieve and Jeff Thomas, "A Question of Honor", *Air Force Times*, March 7, 1994, pg. 12.

2. Forester, Tom and Perry Morrison, Computer Ethics: Cautionary Tales and Ethical Dilemmas in Computing, MIT Press, Cambridge MA, 1994.

3. Gemignani, Michael, "Does Software Copyright Extend to Look and Feel?", *IEEE Software*, March 1987, pg. 90-92.

4. Hafner, Katie and John Markoff, Cyberpunk: Outlaws and Hackers on the Computer Frontier, Simon and Schuster, New York NY, 1991.

5. Johnson, Deborah, "Who Should Teach Computer Ethics and Computers & Society?", *Computers and Society*, vol 24, no. 2, June 1994, pg. 6-7.

6. Martin, James, "Are You Breaking the Law?", *MacWorld*, May 1994, pg. 124-129.

7. Shade, Leslie, Comments on the Feature Article, *Computers and Society*, vol. 24, no. 2, June 1994, pg. 11.

8. Stone, Harold, "Copyrights and Author Responsibility", *COMPUTER*, December 1992, pg. 46-51.

9. Thomas, Jeff, "Values: how they changed", *Air Force Times*, March 7, 1994, pg. 14.