A Course in Computer Ethics for Engineering Students

Author:
C. Rolstad, Oslo University College, Cort Adelersgate 30, 0254 Oslo, Norway. cecilier@iu.hio.no

Abstract — The increasing importance of technology, Internet and computers in society raise new ethical questions which computer engineering students and professionals should be aware of. Nowadays it seems reasonable and necessary to include computer ethics in the engineering curriculum, and when planning a course there are two main issues that should be addressed; ethical questions concerning a profession in computing, and wider questions such as social, economical, legal, philosophical and political implications of the new technology. In a course specific laws and responsibilities connected to the profession should be taught as extensively as possible, -but the issues are continuously and rapidly changing and a second aim should be to provide a frame of reference and perspective, to teach the students reasoning and reflection on the topics. When planning a course in computer ethics, laws and regulations appear to be good material for traditional lecturing, while reasoning and reflection on various topics demands group work, gathering of information, and student presentations. This paper discusses the topics and organisation of such a course.

Index Terms — Code of Ethics and Professional Practice, CyberEthics, Internet.

INTRODUCTION

Cyber comes from the word cybernetics, which according to the online TechEncyclopedia is ‘the comparative study of human and machine processes in order to understand their similarities and differences’. Further it says ‘it often refers to machines that imitate human behaviour’, so called robots. Cyber is extensively used as a prefix and has a similar meaning as virtual. Examples of uses are ‘cyberage’ which means the high-tech era that we are living in today, and ‘cyberattack’ which means an assault against a computer system or network.

As computer and network technology is advancing and becoming available to more of the population we gradually develop into a cybersociety, we shop, do banking, chat, email, and teach on the internet, the computers do the talking for us. ABS car-breaks, microwave ovens, electrical panels for controlling heating and light and so forth are controlled by sensors and micro chips. Thus sensing and the determination of the appropriate actions are left to the machines.

Technology becomes more complicated, incomprehensible and alienated to most people, thus the computer professionals become more important in bridging the gap between machines and humans. Only computer experts can truly understand the capabilities and limitations of the computer systems and they should therefore be able to consider the impact of the cybersystems on the human society. As the society changes new national and international laws and regulation must be introduced. Ethical questions previously addressed when introducing technology as telephone and television needs to be re-examined and also new questions may arise. The impact of humans on cyber systems, as hacking and other types of cyber crime, should also be addressed. We believe a course in cyber ethics will help prepare the computer-engineering students for work in a quickly developing field with a large impact on our society.

Aim of the course

The title of the course is ‘CyberEthics and Social Aspects of Systems’. The course contains two sections: the first is on how computer technology changes society and the second on how to work as a computer professional. The overall aim of the first section is to increase the students awareness of the implications computer technology have on the development of our society. They should realise the responsibility they have as computer professionals to give realistic information about technological possibilities and limitations to the public. They should know pro and con arguments of major issues related to the use of computers and the Internet, and ideally be able to argue orally and in writing. They should be able to ethically evaluate the products of their future employer, whether they work in business, research or education with databases, Internet, programming, numerical modelling or network administration.

The second part of the course deals with working as a computer professional. ‘Social aspects of systems’ was included in the course title to give room for a wider range of topics. These include the development of IT guidelines for companies,
discussions on the effect of company safeguards against cybercrime, the sometimes excessive or obsessive interest for computers which can result in social problems or burnout, and the co-operation and organisation of employers to achieve desirable working conditions and ethical company values. The students should know laws regulating the execution of their profession, be familiar with ethical guidelines as a computer professional, and have knowledge about specialised software for network administrators etc. In practice the student should gain the following through the course:

- ability to argue orally and in writing for pros and cons of central issues of CyberEthics.
- knowledge of specific laws concerning the use of computers.
- knowledge of a code of ethics and professional practice for computer engineers.
- knowledge of relevant software.
- knowledge of how to keep updated on CyberEthical questions.

There are some general effects of the course we hope to achieve. We will put emphasis on two aspects in the course; ethical guidelines for computer professionals and the large impact cyber systems have on our society. One point, which may stem from prejudices, is a common conception of computer engineers as ignorant of the implications computer technology has on our society, they are simply not very interested in it. For comparison, consider a medical doctor, the importance of their work is beyond dispute and the doctors follow ethical guidelines, thus they gain respect in the society. We believe that an increased awareness amongst the students of the importance and impact computers have on our society will motivate the students and improve their self respect. We think that knowledge of laws and ethical guidelines can be particularly useful in conflict situations as professionals, and we think that with experience in arguing and debating cyberethics the computer professionals will become more active in discussions and thus gain more respect in their local community.

TOPICS

Copyright/Intellectual property:

Copyright law protects intellectual ideas and creative work, not only the physical items that are created. To make music, movies, software, books, articles and work of art one needs ideas, knowledge, talent, or one must conduct research and hard labour. The value of these acts should be rewarded, thus we have the copyright law. The US copyright law protects the creators rights to make copies of the work, produce derivative works, to distribute copies, and to perform and display the work in public [1]. As a computer professional it is important to know the law in regard to the production of web pages and software. Ethical discussions on software piracy, the current court case against "DVD-Jon" in Norway [2], and copyright law versus patent protection of software are also relevant topics for the course.

Freedom of speech:

The Internet lets us all be publishers. The technology has changed communications, we have a many-to-many medium where an approval from an editor is not needed. This creates fantastic possibilities, and also quite dreadful adverse effects as for instance the distribution of child pornography. The freedom of speech must be discussed ethically and politically and in regards to the human rights. Topics to be discussed in class are offensive speech, censorship in cyberspace, material inappropriate for children, censorship on the global net, spam, anonymity, and encryption.

Cyber crime:

Computers and the Internet create new possibilities for crime. Typically hacking, fraud, embezzlement, theft, forgery, and industrial espionage are conducted. How can we prevent, detect and prosecute these crimes? How can the crime be fought without constricting the right to privacy and civil liberties? How shall a system administrator act if intrusion on the computer is detected? The questions concerning cyber crime deserves attention amongst computer processinals as the crime is increasing.

Surveillance:

Both cyber crime and other types of crime are investigated and prevented through international police co-operation, for instance the Schengen countries exchange information on criminals through the Schengen Information System (SIS). International data exchange has become necessary as the organised crime across the borders is increasing. Also police forces do not have the same knowledge of the local community as they used to since people are now more mobile. After the terror attack in New York at September 11 the exchange of European data from the SIS has been extended to include the US.
Currently the US is negotiating to get data on European air traffic passengers. The secret Echelon intelligence system of the US, the UK, Canada, Australia and New Zealand, which is believed to monitor most or all types of electronic communication, failed to detect Al Quaida's terror attack on the World Trade Center. It is possible that the amount of data simply was too large. The UK has 1.5 million CCTV cameras and a Londoner is photographed 300 times every day, and yet there are uncertainties on whether these cameras have a crime prevention effect, the criminals avoid the cameras. On the other hand it is certain that law obedient citizens lose their privacy. Increased surveillance of the citizens must be discussed as governments can misuse it, and also mistakes can be made. Computer professionals are, or should be, aware of the large possibilities of mistakes and errors in a system, and therefore promote strict quality control on these systems. They should also be informed of the extent of the use of electronic technology for monitoring all citizens and the resulting loss of privacy.

**Personal data protection:**

National and international data protection laws are developed in response to the increasing use of IT in various transactions. The aims of the laws are to assure that the human rights are followed, especially the right to privacy. An overview of national laws will be given, and furthermore the aims and the scope of the data protection laws, and the relationship between the EU and the US stated in the Safe Harbour agreement will be discussed. It seems that privacy is not very valuable to most citizens, an example is bonus cards in grocery stores where the customers approve the recording of their shopping habits when being rewarded a minor discount. It will be interesting to observe customer’s reactions to the permanent tags on products introduced by the companies Gillette and Benetton, and also to see whether there will be other uses of the tags, for instance for marking patients and equipment in hospitals. Computer professionals are capable of understanding the marketing and surveillance potential that lies in this technology, and should inform the general public.

**Can computer models be used as a base for decisions?**

In research and engineering we use numerical models for many physical applications, some examples are crash tests for cars, dimensioning of constructions, atmospheric circulation models for weather prediction and climate and pollution studies, and ice-flow models for ice age studies. How accurate are these models? Are they giving use better information than actual measurements? Can they give good predictions of the future, and should we make decisions based on these type of results? Many engineering students are likely to work with some kind of modelling, and should be able to evaluate their work and possibly defend it.

**Professional practice:**

The IEEE Computer Society has developed the Software engineering Code of Ethics and Professional Practice, which will be central in this section of the course. Cases that will be discussed in class are copying of an employee’s files, insufficient privacy protection, release of inadequate software or risky systems, and copyright violation. The court case in “Asker og Bærum herredsrett” from 1992 where an employees emails were read by a superior will be used as an example.

**PREMISES FOR THE COURSE**

The course is part of a Master degree in network administration at Oslo University College. The course will be taught in English for international student. Neither the teacher nor the students have English as a mother tongue and this will hopefully create an including atmosphere so that the students will not feel intimidated when participating in group discussions. Students in computer sciences are often used to reading English literature and should therefore be capable of understanding the recommended text.

The students are likely to have a background in science and technology, and therefore we assume that they will not have extensive experience in discussing social and ethical questions as students with a background in social sciences would. We realise that they might need to build up some confidence in this.

Both lectures and group-work sessions will be held in a traditional auditorium with rows of seats facing the lecturer. The seats are mounted to the floor and cannot be moved. The auditorium is well equipped with audio-visual electronics, it has a document camera, TV, video and DVD, PC and laptop that can be connected to the network and displayed on the screen, and microphones and loudspeakers for the lecturer. The lights and blinds are automatically adjusted to the equipment in use.

Computers will be used in the course to some degree. Lecture notes and exercises will be available on the course web page. Multiple choice tests will be used as exercise and for graded tests. Links to relevant web sites will be given, and
the student will use the Internet to gather information. Written work will be handed in digitally. The school is well equipped with students PCs, so it is not necessary that students own a private laptop or PC.

**The course in the European Credit Transfer System (ECTS)**

Oslo University College use the ECTS for crediting and grading courses. One year full work load gives 60 ECTS credits, and a week of 40 hours gives 1.5 ECTS. Grading in the ECTS is either by passed/failed or by five letters from A to E to pass, F for failed. This course will give 10 ECTS credits, which means 6.66 weeks or 266.40 hours of work. The course will be taught over 14 weeks and consist of two lectures and one two-hour group-work session per week. Over the 14 week period the student can then additionally spend roughly two days for self study for this course, or over the total 20 weeks semester they can spend 11 hours or a bit less than 1.4 days per week. The grading for the course will be as passed/failed, and this is further discussed under the section Pedagogical course plan.

**Litterature and videos**

The course will amongst others be using the book ‘A gift of fire’ by Sara Baase [1]. This book provides an excellent overview and discusses relevant topics. Professor Baase is working at the San Diego State University, thus the examples are mainly from the United States. Support literature is the book ‘CyberEthics. Morality and Law in Cyberspace’ by Richard A. Spinello [3]. We need to supply relevant European or other international literature and ‘Data Protection Law, Approaching It’s Rationale, Logic and Limits’ by Lee A. Bygrave [4] will be used when discussing privacy and personal information. Dr. juris. Bygrave is a barrister of the Supreme Court of New South Wales, Australia, and is currently conducting research at the Norwegian Research Centre for Computers and Law. Copies of EU directives and selected international laws will be provided for the students. Support literature in Norwegian may be the prize awarded book ‘Lov og rett i cyberspace’ (directly transacted: Law in Cyberspace) by Inger Marie Sunde, that will be published in autumn 2003. The course will focus on European law only, but students with special interests can investigate any national laws for independently written assignments. In addition recommended literature will be listed, e.g. ‘Secrets & Lies’ by Bruce Schneier [5], and useful web sites will be given on the course web page.

**Pedagogical course plan**

The education at Oslo University College is regulated by the Norwegian law on higher education. This law was reformed in July 2002 and the changes are called “the quality reform”. This reform shall be completely introduced in all Norwegian universities and university colleges by the start of the study year 2003/2004, that is in most cases August. The quality reform introduces several changes such as an extended study year to 10 months, continues feed back to the students during the study year, development of a separate study plan for each student, bachelor and master degrees are introduced, new grading and credit system (see ETCS system above), internationalisation and student exchange, and quality assessment of the education.

When planning the pedagogical structure of the course one has to keep the aims of the course in mind. Ability to argue and knowledge of law, code of ethics and professional practice, relevant software, and how to keep updated on CyberEthics are listed as aims. In addition we want the students to respect and value their role as an engineer more highly, realise what impact computer technology has on society, and become more active in debates concerning Cyberethical questions. In sum the course should offer training in arguing, and information about a set of topics.

So how can one learn to argue well? One must have knowledge about the history of the case, know as many facts as possible, be updated on the latest happenings, know all the sides of the case, in other words the pros and cons, and one must know the vocabulary. If one has all this knowledge the arguing should be a question of formulating ones arguments. Practise in formulating will be developed through written assignments and class discussions. The students will practice with each other and possibly be instructed on taking different sides.

Gaining knowledge about topics can be done in several ways, through traditional lectures, reading, preparing student presentations in class, written assignments, and literature studies. Most courses at the college are taught through traditional lectures, therefore it is desirable to get some variation in the pedagogical methods. The course will therefore be arranged with a mixture of these methods.

The evaluation of the course will be by portfolio assessment. The portfolio can contain a wide range of works, as for instance literature studies, essays, web pages, and reports. The students will be given feedback on their work during the course, so that they can improve it. The feedback will come from peer review from other students. Conducting a peer review is a learning process in itself, evaluating other peoples work makes you reflect over why a piece of work is good or bad. Also
the traditional role where a teacher is the authority will diminish, the students are themselves responsible for the learning process. The peer review will be used only in the initial step when improving the work, not for the final approval of the course work, which will be carried out by the teacher. For the final evaluation the students will be allowed to choose three of their improved works, in addition to a mandatory essay on their development during the course. In the mandatory essay the student shall evaluate their own learning process through the course, such as whether they have gained more self respect as an engineer during the course and whether they are better at arguing about CyberEthics topics. The other three pieces of work chosen should convince the teacher that the student can argue, know some relevant software, know how to keep updated about CyberEthics, and are well informed about the topics. The students will be informed early in the semester that this is partly the aim of the submitted works. The grading of the course will be passed or failed only.

Arranging a course around portfolio assessment provides a pedagogical frame extending far beyond the final evaluation, the students are more active and responsible for their own learning through the whole semester. The student will be told the pedagogical premises in the beginning of the semester, and to some degree participate in setting the premises, we will discuss how one gets better in arguing a case, what makes a written assignment good, and what makes a oral presentation good. They can choose which topics to focus on, they can choose what form of work they want evaluated, and they shall monitor their own development through the course. The peer reviewing fits in very well in this type of course, as the students take on a responsible role by participating actively in evaluating and giving feedback. They will develop skills in critical reading or listening through this process.

As a base for the mandatory self-evaluation essay an exercise will be given before the students have read any literature or discussed any topics. In the first lecture they will answer questions in writing and hand them in. They will first answer a set of quite personal questions like: is an engineer well respected in the society? Do you respect engineers? Why are /are not engineers respected? How does one gain respect? Do you hold any of these character traits or abilities that you mentioned in the previous question? What is your strongest and weakest side as discussed in the previous question? Can you do anything to improve? Do you want to improve? Why/why not? What issues should an engineer know besides technical expertise? Then questions about CyberEthical topics will be asked: What do you know about copyright, freedom of speech, cyber crime, surveillance, personal data protection, code of ethics and professional practice for computer engineers, and how to keep updated on CyberEthics topics? The answers can be handed in a sealed envelope if necessary. The answers will be returned to the student at the end of the course, when they are ready to write the self-assessment essay.

The various topics will be worked through by lectures, discussion groups, and student presentations. There will be written assignments and exercises that must be submitted in order to be entitled to participate in the final portfolio assessment. Also digital multiple choice tests on facts will be given throughout the semester.

**COURSE EVALUATION**

How can we measure whether we have achieved our goals? A web page based survey on attitudes towards the engineers role and the various topics will be developed, and the students should answer them in the beginning of the semester, and after the semester to see whether they have changed their attitudes. Also the students will be asked to answer a course evaluation form. The quality of the portfolio works, especially the self-assessment essay, will give us the answer to several questions, such as whether the student has gained a higher respect for their profession and their role in the society, and if they think it is important to learn about ethical issues.

**CONCLUSIONS**

With the increased use of computer technology and the Internet we think it is important to strengthen the students awareness of the impact computers have on society, and the importance of having a role as an ethical, aware and informed computer engineer. Thus an important aim of the course is to strengthen the student’s ability to argue about CyberEthical topics. A course is planned around portfolio assessment, where students participate actively in deciding which topics and types of work to focus on. Further the students provide feedback to each other by conducting peer review, they carry out a self-assessment in the beginning and the end of the course on their views on the role of the computer engineer in society and on their personal strengths and weaknesses in this regard, as well as on their knowledge to specific Cyber Ethical topics. Finally they evaluate the course so that it can be improved for the next time.

**REFERENCES**


What is ethics doing in a course for software engineers? Like medical, legal and business ethics, engineering ethics is a well-developed area of professional ethics in the modern West. The first codes of engineering ethics were formally adopted by American engineering societies in 1912-1914.  

Professional engineers today, then, are expected to both learn about and live up to ethical standards as a condition of their membership in the profession. 1 Plato, Crito 48b. In Cahn (2010).  

But the average computer/software engineering student might still be confused about how and why this requirement should apply to them. Software engineering is a relatively young practice and compared with other engineering disciplines, its culture of professionalism is still developing. This course introduces the student to the practical imperatives of the engineering profession. With the ever increasing cases of computer crimes, it is important to expose the student with the implications and challenges associated.  

Being a profession that commands a certain way of life, engineering subscribes to fundamental rules that the engineer must adhere to in practice. This course introduces the student to the practical imperatives of the engineering profession. With the ever increasing cases of computer crimes, it is important to expose the student with the implications and challenges associated with use of computers in society today. How Ethics Relate To Computer Crimes


Computer Viruses, Worms, Trojan Horses and Malware Malware refers to software programs designed to damage or do other unwanted actions on computer systems; viruses, worms, Trojan horses, and spyware are the most common types of malware.

LITERATURE REVIEW ON SOFTWARE ENGINEERING FOR COMPUTER GAMES Name: Course: Date Page 1 Abstract Games have often been very common in the past period of time, but with the discovery of computer games, they have penetrated.