Computer Ethics Module Outline

DAY 1	DAY 2	DAY 3	DAY 4	DAY 5
Lesson 1: CURRENT ISSUES IN COMPUTER ETHICS • introduction to ethics • computer crime • hacking • intellectual property • privacy • censorship • free speech *In-class activity* Ethical Worksheet questions	*Lesson 1: (cont.)* CURRENT ISSUES IN COMPUTER ETHICS • specific case studies exploring current issues *In-class activity* Case study articles and questions	*Lesson 1: (cont).* CURRENT ISSUES IN COMPUTER ETHICS • finish in-class activities • introduce debate project • assign project teams and topics *In-class activity* Case study articles and questions *(cont.)*	*Module project:* Computer Ethics Debate • research position • formulate arguments	*Module project:* Computer Ethics Debate • hold debates

Computer Ethics Debate Project

Overview

As a culmination to the Computer Ethics Module, you will have the opportunity to explore your own opinions on the topics discussed during the lesson. You will prepare for a debate discussion on one or more of the following topics: Internet censorship, Computer crime, or Intellectual property. In addition to the readings provided in previous lessons, you should use the resources suggested here, as well as your own research using the Internet, to understand your topics more fully in order to provide more substantial support for your opinions and arguments.

Estimated Time: 2 class periods

Process

You may debate as part of a team, or as an individual, according to your teachers' specifications. Each team or individual will be given a topic (Internet censorship, Computer crime, or Intellectual property) and then will be assigned a position (either *For* or *Against* a specified statement about the topic).

You should spend one class period researching your topic and formulating your argument according to your position. The following class period you will debate your topic against the group/individual with the opposing position. The more research you do, and the more you understand your topic, the stronger your arguments will be. Try to anticipate what your opponent is going to argue, so you can come up with rebuttals beforehand.

Internet Censorship Debate

You will be arguing either *for* or *against* this proposition:

There should be no profanity whatsoever allowed on the Internet.

Issues to consider

The following list contains some questions that will get you thinking about the issues involved in Internet censorship. This is by no means a complete list; feel free to bring in other issues that you think are relevant to your topic.

- What types of things should be considered "profanity"? Do you think that everyone who uses the Internet can agree on a common definition of profanity?
- Who should decide what to regulate? Should it be a responsibility of the government (which government?), Internet Service Providers, individuals who use the web, or some other independent organization?
- Laws exist to prohibit profanity in other forms of media such as radio, television and newspaper. For example, there exists a specific list of words that are illegal to say on the radio. Should the Internet be subject to these same types of laws? Why or why not? What, if anything, makes the Internet different from more traditional forms of media?

Web resources

The Internet Censorship FAQ
A list of frequently asked questions and answers about Censorship – covering both pro and con points of view.
http://www.spectacle.org/freespch/faq.html

American Civil Liberties Union: Cyber-liberties
Provides a list of articles related to Internet censorship laws.
http://www.aclu.org/Cyber-Liberties/Cyber-Libertieslist.cfm?c=59

Electronic Privacy Information Center
Describes current Internet censorship efforts, including links to more information.
http:/www.epic.org/free_speech/censorship/

Hacking Debate

You will be arguing either for or against this proposition:

Hacking should be considered a crime only if it causes harm.

Issues to consider

The following list contains some questions that will get you thinking about the issues involved in hacking. This is by no means a complete list; feel free to bring in other issues that you think are relevant to your topic.

- What, in your definition, constitutes hacking?
- Are some kinds of hacking more acceptable than others?
- What it means to "cause harm". Is something that is illegal always harmful? Can you think of cases where something is harmful but not illegal?
- Are there any cases in which hacking can be useful? If so, is it possible to distinguish these "good" acts of hacking from more harmful cases? How?
- Is it more important to consider the intent of the hacker (i.e. whether he or she intended to do harm) or the consequences caused by their actions?

Web resources

Wired Magazine Article: Hackers Have Rights, Too
http://www.wired.com/news/news/politics/story/20660.html

Interviews about Hacking from CNN.com
Two viewpoints are presented: Hacking is necessary and Hacking is a felony
http://www.cnn.com/TECH/specials/hackers/qandas/

TLC's Discovery Online: Hackers
Extensive information about Hackers and hacking Hall of Fame:
h http://tlc.discovery.com/convergence/hackers/hackers.html..

Intellectual Property Debate

You will be arguing either *for* or *against* this proposition:

> **Internet technology makes copying data fast and easy. Once posted on the web, information should be allowed to be copied or downloaded freely.**

Issues to consider

The following list contains some questions that will get you thinking about the issues involved in intellectual property. This is by no means a complete list; feel free to bring in other issues that you think are relevant to your topic.

- Who benefits from free information available on the Internet? Who suffers?
- Should there be a distinction in the types of information that one is allowed to copy freely? Is some information deserving of more protection that others?
- If copying of information should be regulated or prohibited in some way, how should this be accomplished? What regulations would be fair?
- What types of technologies could be used to stop people from copying prohibited information?

Web resources

CNN.com article: Guarding Intellectual Property on the Internet
http://www.cnn.com/2001/TECH/internet/12/10/intellectual.treaty.idg/

Scientific American article: Who Owns Digital Works?
http://www.library.yale.edu/~okerson/sciam.html

Mp3.com article: Why the Music Industry is Blame for Mp3 Piracy
http://www.mp3.com/news/014.html

Lesson 1: Issues in Computer Ethics
READING

Overview

This lesson introduces some of the ethical issues that current technologies pose to our society. Students will be exposed to topics such as privacy, intellectual property, and censorship and will introduced to the relevant terminology within each of these three topics. Students will then explore the areas of computer related crime, and intellectual property in more depth through reading and discussing a few "case study" articles taken from current events. Note that these articles are from 1999/2000 and you may want to update them.

Estimated Time: 3 class periods

Overview

By the end of this lesson, students should be able to:
- Describe how ethics relates to computing
- Identify several issues related to computer ethics, including privacy rights, intellectual property, censorship, and computer related crime
- Use current terminology when discussing these issues
- Explain some potential threats computer crime poses to society
- Identify some consequences of unlimited MP3 distribution by the Internet
- Defend opinions within the area of computer ethics using research
- Identify counter arguments to opinions on these topics, and explain the complexity involved in many topics concerning computer ethics

Introduction to Computer Ethics

Ethics is a very old subject; people have been debating what's right and wrong for thousands of years. In contrast, computers are new. Modern computing has only existed for about half a century. But computers have raised many new questions about ethics. This handout is a brief survey of some issues in the field of computer ethics.

Computer crime

Computers, and recently the Internet, have created new forms of illegal and dangerous activity. In the news, you sometimes hear about **hackers** – people who use their knowledge of computers to break into systems or steal data[1]. Here are some famous examples of computer hackers:

- John Draper, known by the nickname Cap'n Crunch, figured out how to make free phone calls using a plastic whistle he found in a cereal box in 1972. The whistle made

[1] Actually, computer professionals use the term "hacker" to describe someone who is a clever programmer. Many experts call someone who breaks into systems a **cracker**.

exactly the right frequency to authorize a phone call. This became known as *phone phreaking*.

- In 1988, Robert Morris unleashed a program called the Internet worm, which crashed thousands of computers connected to the Internet. The Internet worm is an example of a **virus**, a program which spreads to many computers, often causing harm.

- Kevin Mitnick was the first computer hacker to have his face on an FBI Most Wanted poster. He has been accused of breaking into systems, stealing credit card numbers and using stolen cellular phone numbers.

Most people would consider the actions of Draper, Morris and Mitnick wrong. But others defend hackers, arguing that they serve a useful purpose by undermining government and corporate secrecy.

Privacy

Especially in the Internet era, privacy has become a major concern among computer users. Banks, hospitals and other institutions hold your private records in databases, making the records vulnerable to hacker attacks and other kinds of snooping. Even as a teenager, your privacy is at risk whenever you use a computer. For instance, should your e-mail address be private? What if someone gets your e-mail address, and uses it to send you e-mail that you don't want to receive? Unwanted e-mail is called **spam**. Spam is becoming a serious problem as more and more people use e-mail.

The privacy issue is often a conflict between law enforcement and individual rights. In 1991, Phil Zimmerman wrote a program called PGP, which he distributed for free on the Internet. PGP allows two people to send each other encoded e-mail messages, making it very hard for a third person to catch the messages and decode them. (This is called an **encryption** system.) In 1993, the US government tried to prosecute Zimmerman, using a law from the 1970's which made it illegal to export encryption programs. Zimmerman argued that PGP was necessary to keep government agencies from reading private e-mail. The Justice Department said that PGP would allow criminals and terrorists to communicate secretly. What do you think? Should ordinary people be allowed to use PGP?

Intellectual property

Whenever you use a program without buying it, you are committing a crime! **Software piracy** is when someone copies a program without paying for it. It is one of the most common and least noticed types of computer crime. Of course, it is extremely tempting for you to copy a friend's computer game instead of buying it yourself. But if thousands of people did that, the programmers who wrote the game would lose money which they deserved. Software companies argue that you would be stealing their **intellectual property**.

Intellectual property is the right to own information. For example, an author owns the rights to his or her book, so it's illegal for you to quote the book without citing the author.

Similarly, a software company owns the code that make up its programs. So it's illegal for you to use those programs, unless you've paid the software company.

The Internet has made it very difficult to keep intellectual property safe. When this curricula was first written in 1999, you could find almost any song in **MP3** format somewhere on the Internet. MP3 is a digital audio format which allows your computer to play CD-quality music. However, many of the MP3 files on the Internet are illegal, because they are the intellectual property of the artist who wrote the song or the record label which sold it. Because of this, the music industry has become very concerned about the illegal distribution and sharing of MP3's on the Internet. Transfer web sites such as Napster and AudioGalaxy have been shut down by law, but new ones are being created.

Censorship and free speech

Nobody controls the Internet, so anyone can put anything they want on the World Wide Web. The web is home to countless adult sites, and many other kinds of questionable content – pages that contain profanity, racist writing or instructions for building bombs. Various countries have passed laws banning certain information from the web. In 1996, the US Congress passed the Communications Decency Act to regulate adult content on the Web. Soon after, the Supreme Court struck it down, arguing that it violated the right to free speech.

Of course, it would be very difficult to regulate the Internet. For one thing, the Internet crosses national boundaries. So if someone puts up a site in America, but it is illegal in Germany or Saudi Arabia, what should be done? Furthermore, there is a distinction between the creators of a web site and the *hosting service* which puts it on the Internet. What if a hosting service puts up a site which is against the law? Should they be held responsible? In 1998, a German judge ruled that CompuServe had broken the law by providing pornographic pictures and Nazi literature – even though CompuServe did not know what kind of content it was making available.

Internet regulation is one of the most hotly debated topics in computers today. What do you think? Should someone oversee the content of the World Wide Web? If so, how should it be policed?

Resources

Learn more about computer criminals at the TLC's Discovery Online Hackers' Hall of Fame: http://tlc.discovery.com/convergence/hackers/bio/bio.html.

The site also has additional information about computer hacking including history, and famous hoaxes: http://tlc.discovery.com/convergence/hackers/hackers.html.

CNN article about a Canadian teenager who was caught hacking into CNN.com and slowing down the site: http://www.cnn.com/2000/TECH/computing/04/19/dos.investigation/

Lesson 1: IN-CLASS ACTIVITIES

Part 1: Ethical Worksheet

1. In one sentence, define the following words:

   a. computer hacker:

   b. virus:

   c. spam:

   d. encryption:

   e. software piracy:

   f. intellectual property:

   g. MP3:

2. Should there be regulations on the Internet (e.g. restricting certain content). Why or why not?

3. Do you think that regulating the Internet would be easy or difficult? Explain.

Part 2: Case Studies

Read the following 2 articles, and answer the corresponding questions. These articles will expand upon your knowledge of computer ethics, primarily in the areas of computer crime and intellectual property.

Article 1: A frenzy of hacking attacks

by Lindsey Arent and Declan McCullagh, Feb. 9, 2000

The Internet is under siege.

In the largest malicious assault in the history of the Net, scofflaws have encircled some of the most popular Web destinations with armies of attacking computers that snarl networks and thwart millions of legitimate visitors.

While this kind of blitzkrieg has been directed at smaller sites in the past, this is the first time that top-tier companies like Yahoo, Amazon, and eBay have come under fire from malicious software that has become steadily more fearsome over the last few years.

The denial-of-service (DoS) war has spread to include CNN, eTrade, ZDNet, and Datek. Both ZDNet and Datek, which said it was offline for 35 minutes, were attacked Wednesday morning.

Keynote Systems, a firm that tracks the reliability of popular Web sites, said within a few minutes of the attack against Amazon that only 1.5 percent of customers who wanted to could enter the site.

Not helping matters is the rush to dot-com glory that has prompted many executives to consider security — and erecting sturdy walls against DoS attacks — an afterthought, instead of viewing it as an integral part of their networks.

Some of the tools apparently used in these wide-ranging assaults, like TFN, Stacheldraht, and trinoo, have been available since last fall, and their progenitors have been used in less-noticed barrages against smaller sites since 1997.

It's not surprising that security experts have anticipated a more serious assault for some time. "The flaws that these people are exploiting are flaws that we have known about for more than five years, which there has been little instance in correcting," says Simson L. Garfinkel, an author and part owner of a security counter-measures firm.

"This is really just the beginning. What we're seeing is as if a group of moral-less teenagers had discovered automatic weapons in an abandoned military site and were going around killing small animals with tremendous firepower," he said.

In this World War Internet, the weaponry is simple and widely available: software distributed in underground areas of the Net that allows a large network of participating computers to overwhelm the target. It's relatively easy to use, though the attacker has to penetrate the security of each of the machines in order to enlist it in the campaign.

The looming threat prompted Carnegie Mellon University's Computer Emergency Response Team to release an advisory last month. Stacheldraht agents have been spotted on Solaris machines, and a version appears to be available for Linux as well.

One big difference — or improvement, if you're the person using it — is that unlike its cousins, Stacheldraht uses encrypted communications to cloak its intentions from administrators who might be monitoring the network.

That isn't exactly heartening news for network administrators at the sites attacked this week. The latest list includes Buy.com, CNN.com, ZDNet, eTrade, and Datek Online Holdings, the No. 4 online broker. "At 7 p.m. EST [Tuesday], we were attacked by hackers," CNN Interactive said in a statement. "A denial-of-service attack occurred until 8:45 p.m. We were seriously affected. We were serving content but it was very inconsistent and very little."

A spokesman for ZDNet said 70 percent of the ZD sites were down for two-and-a-half hours, beginning at 7:10 a.m. EST Wednesday. "We do believe that it was an attack, and it appears to be on the leading brands on the Internet," ZDNet CEO Dan Rosensweig said. Rosensweig says he thinks ZDNet was targeted because of its big-name recognition, but he says he has no idea what's driving the hackers. "The only thing we're sure of is that we're not sure," he said.

Buy.com's site was offline for much of Tuesday, the same day as its successful IPO in which its share price nearly doubled to $25.125 from its asking price.

Details are few. The FBI has tentatively scheduled a press conference for 2 p.m. EST, although companies have released little technical information about who — or what — was behind the mystery fusillade.

Yahoo said that up to 50 different computers hooked up to the Internet were participating, and the rates reached a gigabyte per second — an enormous increase over normal traffic patterns.

Experts said that if history was any indication, the vast majority of unwitting systems that were taken over and are participating in the attack are inside university systems. The reason: Campuses have fast connections to the Internet — necessary to overwhelm sites as large as Yahoo and Amazon — and dorm and faculty computers have notoriously poor security.

The FBI met Tuesday with Yahoo representatives and declined to comment.

Article 2: Can net music be stopped?

by Bruce Haring, USA TODAY, Jan. 26, 1999

The record industry is extremely concerned about Internet piracy of its copyrighted works. Or is it?

Last week, the record industry's main trade group, the Recording Industry Association of America (RIAA), said the future of its members' digital distribution on the Internet was threatened by the proliferation of illegally copied sound files.

The illegal files — known by the nickname given the sound compression system that creates them, MP3 — generally feature songs or entire albums by popular recording artists, all available for free downloading via outlaw Web sites that haven't licensed such rights.

The main battleground in the RIAA's war against MP3 files is currently a lawsuit against San Jose, Calif.-based Diamond Multimedia, maker of a palm-sized portable device that can play back the files once they've been downloaded. The RIAA considers the expansion of the listening options for the free files a serious threat to record sales.

But executives on both sides of the issue are indicating that legal maneuvers may be largely a play for time as the record industry decides the thorny issues posed by a new technology that cannot be stopped.

No organized criminal activity

Pirated records and videos have been around for years. But the Net has the potential of exponentially increasing and vastly simplifying duplication and distribution, making enforcement problematic.

Since it is the first major field of entertainment to face the Internet copying problem, whatever course the music industry's battle takes is likely to set the tone in the future of film, TV and other intellectual property that can be replicated and posted to the Net.

Yet piracy may still be more a potential problem than an actual disaster. The RIAA itself has indicated there is to date no organized criminal activity in Net piracy. The main culprits seem to be college students and computer hobbyists, and that's the focus of the enforcement and education efforts.

It's also hard to pin down how much the current illegal proliferation of sound files is costing the record industry. The RIAA cites large numbers of illegal sites and files on the Net, but can offer few specifics on the number of digital downloads from those sites.

"It's virtually impossible for them to say that most of it is illegal," says Michael Robertson, founder of MP3.com, a site that deals in legal MP3 files, and member of a new MP3 trade group that aims to promote the format and educate the public about its legal uses. "There's simply no way to measure that," he says. "They like to put forth this image of one kid in a college dorm room who sets up a computer and he's just handing out like candy millions of MP3s. It doesn't work that way."

The bandwidth necessary to store large amounts of sound files is costly, Robertson says. If a pirate site goes up, he adds, "Virtually immediately, their ISP is going to spot (the massive use of bandwidth) and shut them down even before the record industry gets to them."

The relative ease of converting compact discs to sound files is fueling the explosion of pirated recordings on the Internet. Each audio CD on the market can have its digital codings easily converted to a sound file. Any number of Internet sites, chat rooms, bulletin boards, file transfer sites and Usenet newsgroups offer software known as a "ripper" to be downloaded for free.

The software converts CD tracks into PC ".wav" files on a hard drive. These files can then be encoded into MP3 files, with stereo sound comparable to that of a CD, and swapped via e-mail, posted on the Net for millions more to download, or "burned" onto a recordable CD disc.

Abundance of legal, illegal sites

The record industry favors compression software that has copyright protections such as encryption and watermarking built in — systems from such companies as RealNetworks, Liquid Audio and AT&T-owned a2b Music. But underground and college-age music collectors have adopted a system from German company Fraunhofer called MPEG-1 Layer 3, or MP3.

Although the format has the ability to offer copyright protections, it has proliferated on the Net minus those standards, leading to an abundance of sites both legal and illegal.

"The fact is that you can keep taking them down, but they can keep popping back up, because absolutely anybody with a CD-ROM drive in a computer can become a publisher," says RIAA general counsel Cary Sherman. "It's just very difficult to track down and bring actions against all those people who are doing this on a worldwide basis."

Even as the RIAA complained, some of the entertainment industry's leading executives were airing a different point of view. Time Warner CEO Gerald Levin (whose company owns record labels Atlantic and Elektra) and Seagram vice chairman Robert Matschullat (close to closing a deal that would unite Universal Music and PolyGram to create the world's largest record company) minimized the threat of Net piracy in speeches at a closed media and entertainment conference run by investment group Bear Stearns in Palm Springs, Calif., according to attendees. Copying has always existed, attendees quoted Matschullat as saying, and both were eager to proceed with plans for digital distribution.

A U.S. District Court judge ruled late last month that Diamond Multimedia could start selling its portable Rio MP3 player. A trial on the larger issue — whether the device violates the Audio Home Recording Act's prohibition against devices capable of generating multiple copies of digital recordings — still must be held.

Effectively, the judge has allowed Diamond to get Rio to market in time for the holidays. Samsung also plans to market a portable MP3 player, and other electronics makers are said to be readying similar devices.

"If MP3 devices without protection proliferate, then I think it retards the entire market for digital distribution, because it's going to be very hard for companies that protect the content to compete with the free music that would be available online," Sherman says. He called for cooperation between the record industry, Internet companies and the consumer electronics industry to achieve such protections.

"MP3 is unstoppable"

Yet some artists and record labels are already forging ahead, in the belief the popularity of MP3s could generate a huge promotion for sales of their legitimate recordings. Such major labels as Disney-owned Hollywood Records (Alien Sex Fiend), Mercury (Swirl 360) and the Beastie Boys' own Grand Royal label have already distributed free songs in the MP3 format.

Other record industry veterans say the business needs time to adjust, get its pricing and marketing plans together, and brace employees and customers for the roiling effects sure to come from a sea change in the business.

"I think that the industry is not as concerned about (piracy) as sometimes they let on to be," says Jim Griffin, the founder of consulting firm OneHouse and a former executive at Geffen Records. The future is about "persuading people to buy your product," not forcing them to accept certain delivery formats, he says. And the marketing muscle of record corporations with multinational financial backing is perfectly positioned to take advantage of the Internet.

Bob Kohn, co-founder of the GoodNoise music sites, says the RIAA "is pitting themselves against independent record labels and aspiring recording artists who have a new, exciting alternative means of distributing their music. The cat's out of the bag, the horse is out of the barn, and the toothpaste is out of the tube. MP3 is unstoppable."

Eventually, consumer demand will push digital distribution, and anyone who wants to stay in the game will adjust, says Marc Geiger, co-founder of the Lollapalooza festival, who now runs the Ultimate Band List (www.ubl.com).

"When VCRs were coming out, the theater industry thought they were going out of business," Geiger says. "What happened? They doubled their business. The record companies are the theater business right now."

Case study questions

Base your answers to questions 1-5 on *Article 1: A Frenzy of Hacking Attacks*

1. Name four sites that were attacked by the hackers.

2. What problems did Amazon have because of the attack?

3. What tools did the hackers use to attack the sites, and where did they find those tools?

4. Where did the hackers find those tools?

5. In your opinion, why do you think that someone did this?

Base your answers to questions 6-10 on *Article 2: Can Net Music Be Stopped?*

6. Why is the music industry concerned about MP3's?

7. Who is responsible for most music piracy on the Internet?

8. Why is it hard for the music industry to stop MP3's?

9. Briefly describe what you think the opinions of the following stakeholders would be on the issue of free MP3 trading on the Internet:
   The Music Industry (business people who run major record labels):

   The Artists (musicians who write and perform the songs):

   The Consumer (the fan who wants to listen to the music at home):

In your own opinion, is it wrong to freely trade MP3's over the Internet? Why or why not?