Third AP Edition

Java Methods

Object-Oriented Programming and Data Structures

Maria Litvin
Phillips Academy, Andover, Massachusetts

Gary Litvin
Skylight Software, Inc.

Skylight Publishing
Andover, Massachusetts

Skylight Publishing
9 Bartlet Street, Suite 70
Andover, MA 01810

web: http://www.skylit.com
e-mail: sales@skylit.com
support@skylit.com

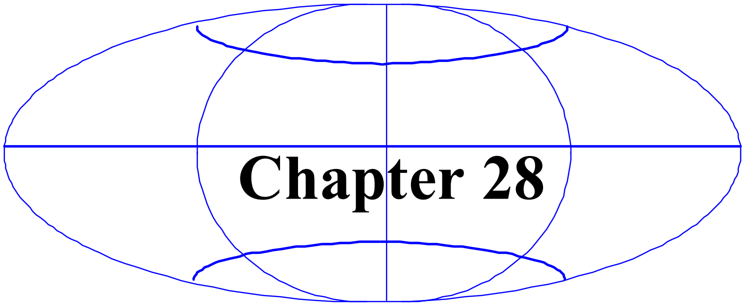
Library of Congress Control Number: 2014922396

ISBN 978-0-9824775-6-4

[*] AP and Advanced Placement are registered trademarks of The College Board, which was not involved in the production of and does not endorse this book.

The names of commercially available software and products mentioned in this book are used for identification purposes only and may be trademarks or registered trademarks owned by corporations and other commercial entities. Skylight Publishing and the authors have no affiliation with and disclaim any sponsorship or endorsement by any of these product manufacturers or trademark owners.

Oracle, Java, and Java logos are trademarks or registered trademarks of Oracle Corporation and/or its affiliates in the U.S. and other countries.



Chapter 28

Computing in Context:

Creative, Responsible, and Ethical Computer Use

28.1 Prologue

When early humans harnessed the power of fire, they found it kept them warm, helped prepare their food, and kept wild beasts at bay but could also burn down their huts or rage uncontrollably as a forest fire, destroying everything in its path. Humans have been playing with fire ever since. Technological progress has brought new benefits but also new dangers and fears. For instance, advances in nuclear physics promise unlimited sources of cheap energy. But they also threaten to pollute our planet with nuclear waste or destroy it completely in a nuclear war. Advances in chemistry, biology, and medicine are helping eradicate devastating diseases, develop new life-saving drugs and vaccines, and increase food production. But they have also brought pollution, large-scale production of brain-damaging drugs, and hideous chemical and biological weapons. Computer technology seems pretty harmless by comparison: bits and bytes flipping inside tiny silicon chips. But is it?

In the second decade of the twenty-first century we are still at the very dawn of the computer era. What will it bring us? This technology goes to the very core of humanity: the human mind, the way we acquire and process information and communicate with each other. Will computers help make us safer, better informed, or more free? Or will we become a population of networked slaves, duped by misinformation, serving an invisible master? As science-fiction authors have imagined the worst, professional ethicists and system developers have thought a great deal about how to keep it from happening. Issues of responsible computer use, computer ethics, security, and privacy have been in the foreground since the first computers were built. This field of inquiry, in fact, is much broader and more complicated than computer technology itself. In this brief overview we can only give you a glimpse of the many complex issues involved.

The first difficulty is the newness of the field. The use of more traditional technologies is governed by laws and ethical principles accepted in a community and transmitted from the elders to new generations. Computer technology, however, is developing and changing so fast that laws have been unable to keep up and customs and traditions have had no time to develop. Right now it is the younger generation, the teenagers, who have the most experience and savvy in using computers and the Internet. Your parents most likely cannot teach you ethical computer behavior or good Internet manners. You are on your own, and you are holding the future in your hands.

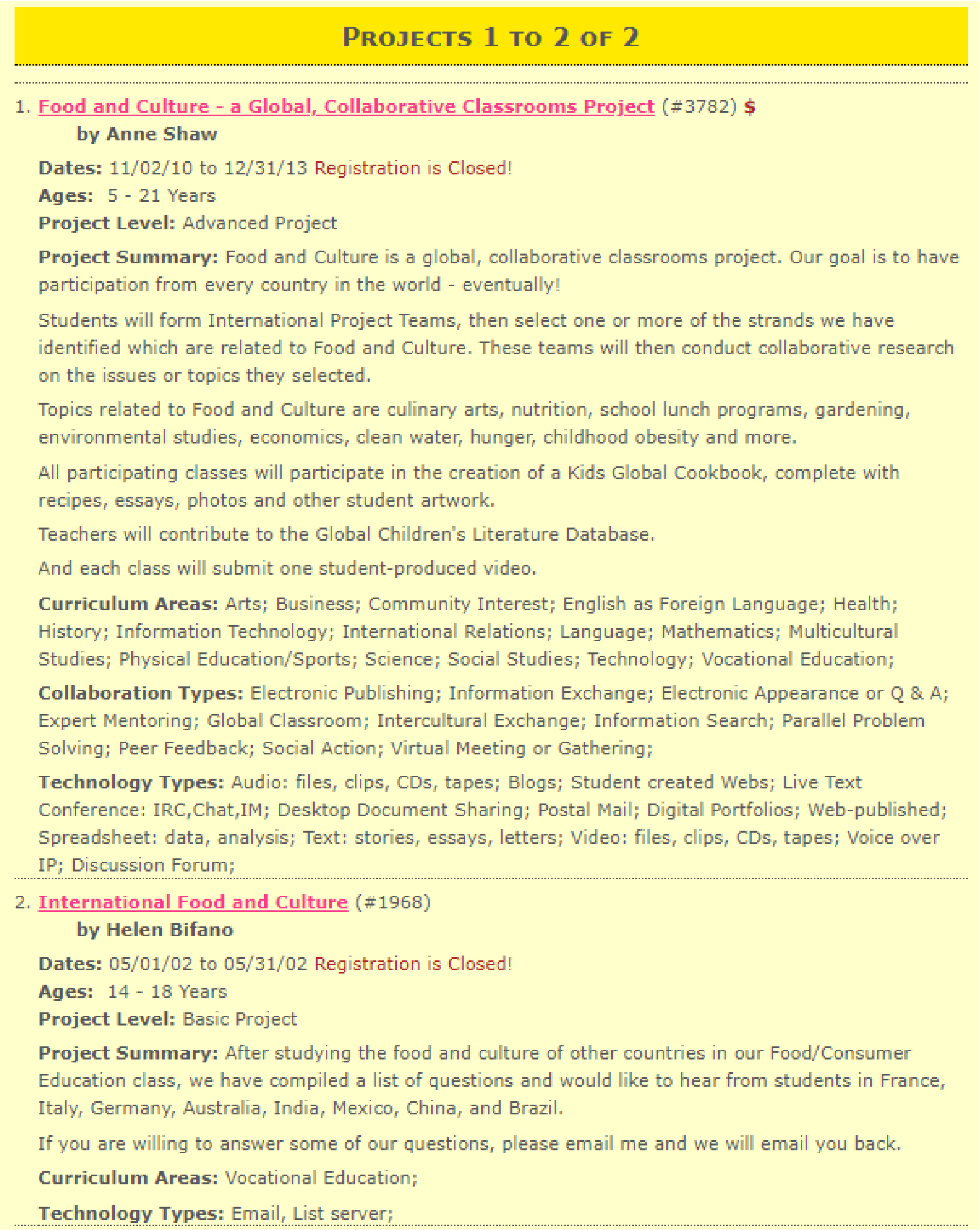
Another problem is that cyberspace is the first truly global phenomenon. It has no boundaries, no tariffs, no customs inspectors, no immigration visas. The distance between point *A* and point *B* in cyberspace is measured only by common interest, opinion, and intent.

Of course, this allows inter-regional and international collaborative projects of unprecedented speed and scale. However, like any society, the global society of Cyberspace has its "bad guys." A malicious computer virus released in a remote country can reach computer systems all over the world in seconds. A user in the United States can log into online gambling or pornography sites located halfway around the world. The Internet unites communities and countries with different legal systems, different customs and cultures, and different languages. How do you go about developing universal legal and ethical codes for half of the world population?

28.2 Be Creative!

A computer is a versatile tool; your job is to learn how to use it judiciously and harness its power to benefit people. A computer connected to the Internet is a universal communications device. Your job is to learn how to explore the digital world, connect to and collaborate with others, and make a positive difference in the real world. Here are some ideas and resources that will you help you on that journey.

1. Explore some "collaborate now" projects on `globalschoolnet.org`. Choose a current or archived project that interests you. Figure 28-1 offers an example. Follow the link to the project details, study the setup, and confirm your interest. Create a brief online journal, a PowerPoint presentation, or a video that will explain to your classmates and teachers what the project is about. Explain why the project you selected is important, meaningful, and relevant in today's world. After getting approval from your teacher, form a small team of your classmates interested in working with you on the project. Learn what has been done so far and the tools necessary to collaborate with your peers around the world: making blogs, audio files and video clips, spreadsheet data analysis, and so on. Learn and help your teammates master these tools. Make periodic presentations about your progress and the status of the project to your class.



PROJECTS 1 TO 2 OF 2

1. Food and Culture - a Global, Collaborative Classrooms Project (#3782) $

by Anne Shaw

Dates: 11/02/10 to 12/31/13 Registration is Closed!
Ages: 5 - 21 Years
Project Level: Advanced Project

Project Summary: Food and Culture is a global, collaborative classrooms project. Our goal is to have participation from every country in the world - eventually!

Students will form International Project Teams, then select one or more of the strands we have identified which are related to Food and Culture. These teams will then conduct collaborative research on the issues or topics they selected.

Topics related to Food and Culture are culinary arts, nutrition, school lunch programs, gardening, environmental studies, economics, clean water, hunger, childhood obesity and more.

All participating classes will participate in the creation of a Kids Global Cookbook, complete with recipes, essays, photos and other student artwork.

Teachers will contribute to the Global Children's Literature Database.

And each class will submit one student-produced video.

Curriculum Areas: Arts; Business; Community Interest; English as Foreign Language; Health; History; Information Technology; International Relations; Language; Mathematics; Multicultural Studies; Physical Education/Sports; Science; Social Studies; Technology; Vocational Education;

Collaboration Types: Electronic Publishing; Information Exchange; Electronic Appearance or Q & A; Expert Mentoring; Global Classroom; Intercultural Exchange; Information Search; Parallel Problem Solving; Peer Feedback; Social Action; Virtual Meeting or Gathering;

Technology Types: Audio: files, clips, CDs, tapes; Blogs; Student created Webs; Live Text Conference: IRC,Chat,IM; Desktop Document Sharing; Postal Mail; Digital Portfolios; Web-published; Spreadsheet: data, analysis; Text: stories, essays, letters; Video: files, clips, CDs, tapes; Voice over IP; Discussion Forum;

2. International Food and Culture (#1968)

by Helen Bifano

Dates: 05/01/02 to 05/31/02 Registration is Closed!
Ages: 14 - 18 Years
Project Level: Basic Project

Project Summary: After studying the food and culture of other countries in our Food/Consumer Education class, we have compiled a list of questions and would like to hear from students in France, Italy, Germany, Australia, India, Mexico, China, and Brazil.

If you are willing to answer some of our questions, please email me and we will email you back.

Curriculum Areas: Vocational Education;

Technology Types: Email, List server;

Figure 28-1. Food and Culture projects at www.globalschoolnet.org

2. Google “Doors to Diplomacy” and learn about this project and competition, sponsored by the U.S. Department of State. Select one of the past projects that received an award or an honorable mention. Arrange with a teacher to make a presentation about it to a social studies or history class at your school or at one of your town’s middle schools.

3. Visit your school’s web site with a critical eye. Learn about the tools that were used to create it — interview the webmaster or technology coordinator at your school. Create a list of suggestions for improvement, writing justifications for your proposed changes. Try to learn the tools necessary to implement the changes.

4. Interview an English, Math, Science, or Social Studies teacher or the teacher of your own computer science class about the topics to be taught in the class in the near future. Then collect information about these topics from textbooks and the Internet. Create a computer game, such as Jeopardy, a quiz in the style of `freerice.com` [1], or a crossword puzzle [1] for that class. With your teacher’s approval, organize a competition in which your peers will vote for the best product. Offer the best games and puzzles to teachers of the corresponding subjects to try out in their classes.

5. Visit the National Center for Education Statistics web site [1] and under the “Data & Tools” tab select “Custom Datasets & Tables.” Learn how to download statistical data in the CSV (Comma Separated Values) format and import them into a spreadsheet. (Pay attention, of course, to the data use Terms and Conditions.) Design a meaningful study based on the relevant data that would compare your state or area statistics with nationwide data. Design a way to present your findings in interesting tables, graphs, and charts (find appealing examples and guidelines for presenting statistical data on the Internet). Publish the results in a blog, journal, or on a page on your school’s intranet.

6. Choose a topic of interest (examples could include a particular sport, patterns of using Facebook, Twitter, or texting, demographics and census data for your state, financial data, and so on). Use an Internet search engine to find a reliable source of statistical data for the chosen topic. (Pay attention to the data use Terms and Conditions.) Import the data into a spreadsheet or another statistical analysis tool or write your own program to perform custom pre-processing of the data. Extract meaningful relevant statistics and present your results in PowerPoint with appealing graphics.

7. Form a team of your classmates to participate in the M^3 (Moody's Mega Math) Challenge competition [1] and convince one of your teachers to coach your team. Don't be put off by the math: the contest is about finding, organizing, and analyzing data and solving meaningful real-life problems. For example, the 2020 challenge problem was "Keep on trucking: U.S. big rigs turnover from diesel to electric." From Siam's web site:

   > The problem asked teams to create a model to predict what percentage of semi-trucks will be electric in the next few years and decades, determine the number and locations of charging stations along major U.S. trucking routes that are needed for an all-electric trucking industry, and to prioritize which routes should be developed with electric charging infrastructure first.

   The winning papers from previous years are available on the M^3 web site; the winners receive substantial scholarship prizes.

8. Locate on the Internet several images related to an academic subject (for example, Fibonacci numbers in nature, or rain forest management in Brazil). Using Photoshop or other image processing software, make a poster on the subject (of course, don't forget to credit the sources of the images).

9. Create a project in Scratch [1], demonstrate it to a group of elementary or middle school children in your school district, and explain how it was put together.

10. Learn the Processing programming language, which is based on Java [1]. Download the software and study the online tutorials and examples available on the Processing web site. Individually or with a small team of classmates, design an art project and implement it in Processing. Visit the Processing wiki and discussion forum to ask for advice, share information with other users, and see their work. Also consult your art teacher. Present your work in a small exhibit of computer art created by students.

11. Are math teachers in your school familiar with GeoGebra [1]? It is an excellent free software product for teaching mathematics, from algebra and geometry to calculus. Learn how to use it for doing some of your math homework. If a teacher in your school is not familiar with GeoGebra, offer to give a demo and help with learning how to use it.

12. Individually or with a group of your classmates, get involved with the OLPC (One Laptop per Child) developer program [1]. Research what has been done and propose a project. (If your project is approved, you will receive a free XO laptop for development.) Work with volunteer mentors and eventually become one.

13. Organize a debate with your classmates or your school's debate club on Digital Rights Management (DRM) or a high-profile case that involved the acquisition and use of digital information (for example, Wikileaks, the case of Aaron Swartz, or Henk Krol, a member of the Dutch parliament). In preparation for the debate, find reputable sources for news and opinions on the Internet. Was the information acquired legally? Was it ethical? Was the information used for a good cause? Was sharing of the information legal? Your teacher or a jury will judge your debate team based on how informed you are and how convincing your arguments are. Compile and present a bibliography of the sources you used in the debate.

14. With your classmates, create a digital or physical exhibition (posters) on the history of computers and the Internet. Include exhibits on computer pioneers, early computers, the history and evolution of programming languages, milestones in hardware from mainframes to smartphones, women in computing, Moore's Law, and current computer and Internet use around the world, to name a few. Include, of course, appropriate attributions to the web sites, books, and photographs that you used. Examine copyright laws applicable to such displays and request any permissions needed to use the materials.

15. Create a digital survey on your school's intranet or on Survey Monkey [1] to study how much time students in your school spend doing homework, playing sports, watching TV, playing video games, using social networks, and texting. Do some research on the Internet to find the national averages, too. Enter your results into a spreadsheet organized by grade and gender. Create appropriate and visually appealing charts, and post your report on your school's intranet or on the Internet.

16. Help organize a mini-conference on Computers and Society. Your peers and teachers would be among the panelists and presenters. Sample topics for discussion:
    - Social networks: real human connections?
    - The future of education: virtual schools and Massive Open Online Courses (MOOCs)
    - Journalism in the digital age
    - Music in the networked world
    - Video games: innocent entertainment or a path to violence?
    - Copyright and free information exchange
    - Democracy and civic action in the Internet age

❖ ❖ ❖

The above examples are just a small sample of the possibilities: the connected world offers limitless opportunities to share information and work with others on meaningful and relevant projects. Your work will speak for itself, and you will be proud of it!

28.3 Rules of Digital Citizenship

28.3.1 Formulating Ethical Guidelines

As in any other science and technology field, trained computer experts have a great deal of power to decide whether this technology will be used for good or for evil. Many professions, including doctors, lawyers, and civil engineers, have developed codes of conduct to describe the ethical and responsible behavior that defines a professional. They have also developed licensing requirements, which can include some set of knowledge as well as adherence to a professional code of ethics. The oldest professional code, the Hippocratic Oath [1], was written around 400 BCE, but its principles are held sacred by physicians to this day.

Until recently, the computer software profession was considered too technical or arcane to develop its own code of ethics. This is beginning to change. Professional societies have been developing and publishing codes of conduct for computer professionals.

Years ago, The Association for Computing Machinery (ACM) developed a General ACM Code of Ethics and Professional Conduct [1] and a Software Engineering Code of Ethics and Professional Practice [1]. ACM is the oldest and largest organization for computer professionals in the world. Founded in 1947, it has over 100,000 members from 190 countries. In the introduction to this code, the ACM/IEEE-CS Joint Task Force on Software Engineering Ethics and Professional Practices states:

> "To ensure, as much as possible, that their efforts will be used for good, software engineers must commit themselves to making software engineering a beneficial and respected profession. In accordance with that commitment, software engineers shall adhere to the following Code of Ethics and Professional Practice…"

The ACM's Software Engineering code includes the following general principles and professional responsibilities:[*]

1. Contribute to society and to human well-being, acknowledging that all people are stakeholders in computing.
2. Avoid harm.
3. Be honest and trustworthy.
4. Be fair and take action not to discriminate.
5. Respect the work required to produce new ideas, inventions, creative works, and computing artifacts.
6. Respect privacy.
7. Honor confidentiality.
8. Strive to achieve high quality in both the processes and products of professional work.
9. Maintain high standards of professional competence, conduct, and ethical practice.

Many web sites have collections of links to other codes of ethics, as well as courses, papers, case studies, and other educational recourses (see, for example, [1, 2, 3, 4]).

[*] Copyright (c) 2018 by the Association for Computing Machinery, Inc. and the Institute for Electrical and Electronics Engineers, Inc. This Code may be republished without permission as long as it is not changed in any way and it carries this copyright notice.

28.3.2 Maintaining Professional Standards

Professional licensing is a formal procedure, usually mandated by the state government. Its purpose is to ensure public safety, health, and welfare, and to protect consumers. Certification is usually voluntary; it documents the completion of a course of study and/or passing a certification exam. Professional licensing is common in many professions: civil engineering, accounting, the medical professions, and teaching. Licensing is often called certification, too.

The idea of certifying software professionals has run into many difficulties and faces some objections from the professionals themselves. The main difficulty is posed by the rapid changes in the field and the narrow specialization of the software professionals. It is hard to formalize what constitutes professional competence and even if one manages to do that, the formula may change drastically in just a few years. Proponents of certification point out that certification can still test core professional knowledge, including computer ethics and responsible computer use.

ACM started a certification program in the early 1980s, but abandoned it later due to the lack of interest and resistance among its members.

At the national level, the most influential professional organizations for certification of software engineers are the Institute for Certification of Computing Professionals (ICCP) and IEEE (the Institute of Electrical and Electronics Engineers, pronounced Eye-triple-E). ICCP offers certificates for several subspecialties of software engineering [1]. IEEE offers Professional Software Developer Certification [1].

Most successful certification programs, however, are managed by software companies themselves and are geared towards specific software technologies that these companies offer. Microsoft, for example, has a number of certification programs [1], including Microsoft Developer and Microsoft Data Engineer. Oracle Academy has many narrowly specialized certifications in Java software development for students and professionals [1].

28.3.3 Regulating Users

Apart from ethical issues for computer professionals, there are ethical rules and acceptable use policies for computer users. Almost every school, college, and company has established a set of rules for using its computers and networks. A typical set includes rules for maintaining system integrity, rules against storing, posting, or e-mailing obscene or offensive material, rules against downloading copyrighted material, and a ban on exceeding allocated bandwidth by downloading or sending excessive amounts of data via the organization's LAN or WAN. Users are prohibited from intentionally introducing computer viruses, hiding their identities or impersonating other users, spreading chain letters, and so on. Refer to your school's acceptable use policies. The acceptable use policy may also define the user's right to privacy and stipulate the organization's right to monitor communications and system access by its students or employees.

However, no set of rules and regulations can replace general politeness and common sense. Just like in other areas of life, computer and especially Internet users should develop a kind of etiquette, a set of good manners for dealing with others. *Netiquette*, or good manners in Internet use, are widely discussed on the web. A Google search for "netiquette" returns over 17,800,000 hits! A good place to start is "netiquette Home Page" [1]. See also `netmanners.com` [1]; you can join discussions there.

As in any etiquette, the most important rule is to remember that there are human beings on the receiving end and to care about them. Here is a famous quote from the Irish political philosopher Edmund Burke (1729-1797):

> "Manners are of more importance than laws. Manners are what vex or soothe, corrupt or purify, exalt or debase, barbarize or refine us, by a constant, steady, uniform, insensible operation, like that of the air we breathe in."

28.4 System Reliability and Security

To most casual computer users, system security and reliability mean keeping their computer virus-free and backing up their files once in a while. We rarely think about the enormous problem of maintaining the security of computer systems and networks. In a developed country, computers run military and civilian communication systems, utilities (electrical grids, water purification plants, etc.), financial institutions (banks, brokerages, stock exchanges, etc.), space exploration systems, medical records and patient monitoring systems, industrial facilities, online commerce, media, document archives, and so on. All these systems are vulnerable to malfunctions, sabotage, or terrorism; yet they need to provide uninterrupted service and maintain the integrity of data.

28.4.1 Avoiding System Failure

Even in the absence of malice, hardware and software reliability pose huge problems for developers. A system's overall complexity and the interdependence of its components sometimes exceed the ability to test and manage them effectively. Anecdotes abound of major failures and losses caused by tiny errors in software code.

The costs of system failures to businesses can be staggering [1]. According to a 2011 study by CA Technologies [1], businesses lost $26.5 billion in revenue each year due to unplanned IT (Information Technology) downtime. A brokerage firm might lose millions of dollars per hour!

One of the early projects on fault-tolerant computers was sponsored by NASA's Jet Propulsion Laboratory (JPL) in the 1960s. JPL invited Algirdas Avizienis, a researcher from the University of California, Los Angeles, to develop a fault-tolerant computer system for use on long space missions. In those days, computer failures occurred much more frequently than now. A computer on board a deep space mission could not afford to fail. Avizienis named his computer design STAR, for Self Testing and Repair. The reliability of the STAR computer was achieved by integrating several redundant duplicate versions of each subsystem [1].

All mission-critical applications employ some level of redundancy: uninterruptible hot-swappable power supplies, multi-path input/output adapters, and so on. But hardware alone cannot assure reliability. To operate without failures, a reliable system must have trained personnel available and sound management and control procedures in place. There are experiments in fault-tolerant software, too. For instance, the same critical software module may be implemented in two versions by two independent teams of developers, then run in parallel on two systems that compare the computation results at critical junctions.

28.4.2 Maintaining Data Integrity

Another aspect of system reliability is the problem of maintaining data integrity in large databases and data archives. Electronic data is often the most valuable asset in an enterprise. The integrity of data is achieved through established back-up procedures and data validation.

Digital data archives pose their own problems: besides protecting data repositories from physical damage, the data must be protected from obsolescence and what is known in the industry as "bit rot" or "bit decay" [1]. The optical or magnetic media that store the data have a limited life span; the data must be periodically reproduced on new devices and in new formats that are currently in use.

28.4.3 Protecting Secure Systems and Databases

The Internet has brought tremendous benefits and empowered millions of people. It has also become a stage for unethical and criminal activity of staggering proportions around the world. Before the advent of the Internet, computer crime was rare and fairly exotic: a particular incident would be remembered for years. Unfortunately, today cybercrime has become routine. No wonder experts in computer security have become the most sought-after information technology (IT) professionals.

Software engineers try to design their systems to be easy to use and efficient; security is not always on their minds. It takes a criminal mindset to find and explore vulnerabilities in software. These vulnerabilities are often fixed only after they have been exploited.

To most of us, system security appears in the form of antivirus software and passwords we use to log into web sites for e-mail or shopping. But computer system and network security is a much larger problem. Security is essential in military applications, financial and business systems, e-commerce, law enforcement, and other areas. Security issues include physical protection for computer systems and data storage, secure access to data, and secure communications.

Computer security has two sides. On one hand, large organizations have to protect their computer systems, networks, and databases from malicious individuals. On the other hand, individual computer users have to protect their computers from viruses and other malicious software, known as "malware."

The security of systems that give access to many subscribers or customers — banks, e-commerce web sites, medical databases, social networks, and so on — is a much more difficult problem. These systems must keep track of thousands or millions of users and keep their accounts secure. The most common way for a user to protect access to his or her account — just about the only way used at the present time — is a user name and password. A typical user uses dozens of passwords at different web sites (or the same one — not a recommended practice). Many organizations impose requirements on a password to make it more secure: it must be at least so many characters long, must have letters and digits, and so on. Some organizations require the user to change the password every few months. All of this is not very convenient for an average user, but the user has little say in how things run.

Password protection works, by and large, but it is not one hundred percent secure. A password can be guessed or stolen. A user may simply write it down on paper or in an unsecured computer file. A more common situation is when the user's computer is infected with malware that eavesdrops on the user's activities and sends private information, including user names, passwords, and credit card numbers to criminals. Web sites often provide tools for recovering a forgotten password, such as security questions, emailing password reset information to the user, and so on. These procedures are often less secure than the password itself, and can be easily "hacked." More recent reports have described attempts to steal a password entered on a smart phone by capturing vibrations. A few years ago a group of researchers demonstrated a way of extracting and decrypting private data from an Android smartphone by literally freezing it [1].

Stolen passwords are especially damaging when they involve system managers with high access privileges. Even very experienced database administrators may become victims of sophisticated "phishing" attacks, in which a malicious email message is disguised as a legitimate message from a friend or supervisor. The message instructs the reader to follow a link that installs malware on the user's computer, which eventually collects passwords and other private information. Alternatively, a dishonest employee can learn an administrator's password by illicit means. After getting access, the hacker can potentially steal millions of records with confidential customer information and sell them to criminal organizations. Or he can tamper with the data to his advantage. For example, the 2020 hack of Blackbaud, a fundraising database services provider for non-profit organizations, gave criminals access to personal information of millions of donors and potential donors of major non-profits, including hundreds of schools and colleges. Blackbaud agreed to pay a hefty ransom in exchange for criminals' promise to destroy the stolen data.

An alternative to password-based security would be a user authentication system based on physical devices, voice, biometrics, fingerprints, signatures, keystroke patterns, face recognition, and so on. These ideas are the subject of research; all have vulnerabilities. According to a 2013 BBC News report [1], a Brazilian doctor was arrested with six silicone prosthetic fingers, which she used to fool a biometric employee attendance device to cover up for absent colleagues. More recently, a hacker cloned a German politician's fingerprint from photos taken with an ordinary camera at a press conference [1].

In addition to protecting access to databases and computer systems, data has to be protected when it travels between users and servers. This is accomplished through encryption. Even so, hackers can attempt to tamper with the data before it is encrypted. A typical user interacts with web sites through a browser, which displays information in a convenient GUI format. But a sophisticated user can eavesdrop on the data sent to and received from the server, bypassing the browser. In fact, there are software tools on the market that facilitate eavesdropping on your browser and tampering with data (for example, the Tamper Data add-on for Firefox browser, [1]). A malicious user can send tampered-with data to the server for which the server may be not prepared, and use back-end software vulnerabilities to his advantage.

So we are witnessing a continuing battle between security specialists and criminals, who are finding new ways to subvert systems and trick computer users, find and exploit new vulnerabilities, get around virus/malware detection software, steal confidential information, and perpetrate fraud. Most users these days have antivirus software installed on their computers, but many users fail to update it regularly or become victims of "phishing" scams. Criminal enterprises spread computer viruses and hijack thousands of computers, forming "botnets" of virus-infected computers. These computers relay spam and can be used to launch a denial-of-service attack.

Launching computer viruses and breaking into secure systems is not only unlawful; it is also unethical. Unfortunately, talented computer enthusiasts sometimes consider it a badge of honor to launch a new virus or to "hack" into a secure system or web site. The same person would never enter your home without permission; but, for no obvious reason, a hacker considers it okay to break into a computer system, often causing panic and millions of dollars in damage. A group of loosely affiliated hackers called Anonymous resorts to similar unlawful tactics — not to seek financial gain but, purportedly, to promote various causes of their choosing.

28.5 Legal Issues

The rapid emergence of Cyberspace has posed difficult questions for lawmakers and legal experts. The existing laws for protecting security, privacy, and intellectual property rights are not always applicable to the new environment. They have to be reinterpreted and extended, and new laws must be written. More importantly, laws ultimately reflect the prevailing customs and practices of their community. But with cyberspace, a new community has emerged that has no national borders and no traditional customs. The overwhelming majority of people in this community are children or teenagers. This new generation of computer users is creating new customs and practices that will eventually be codified in law. Therefore it is important that this new Internet generation be better educated in the value of the rule of law, the application of existing laws, and the concepts of ethical behavior and responsible use.

The legal issues in cyberspace that have generated most debate are privacy, freedom of expression versus censorship, and intellectual property rights. As the recent debate has demonstrated, these are complicated issues on which thoughtful people can sometimes disagree.

28.5.1 Privacy

Over the past several decades, judges and constitutional lawyers in the United States have come to recognize a “right to privacy” as one of the fundamental rights guaranteed by the first ten amendments to the U.S. Constitution. This right, enshrined and expanded in several landmark decisions of the U.S. Supreme Court, means that a government agency must show it has a “compelling state interest” before it can intervene in a citizen’s personal affairs. The requirement for employers is similarly strict.

At the same time, as technology in developed countries gets ever more sophisticated, the expectation of actual privacy is becoming more and more unrealistic. In any developed country, there are hundreds of computer records for nearly every citizen. In the United States, the federal and state governments keep social security records, tax records, and driver’s license and motor vehicle registration records. Insurance companies keep insurance policies and health records. Credit bureaus keep credit card and mortgage records. Banks and investment firms keep financial records.

Clinics and hospitals keep health records. Utility companies keep your account records, including a record of every phone call you make. Your every e-mail may be archived on several computers. Every web site you visit is logged in a server log somewhere. If you go on a shopping spree at your favorite mall and your credit card processor is alerted to the unusual spending, a fraud agent can track you in real time as you go from store to store charging purchases.

Who has access to all this information? "Authorized personnel" — that is to say, thousands of government and private sector employees. Is this information secure? We can only guess.

Each citizen of the real world has an electronic incarnation in Cyberspace. In the last several years, "identity theft" has become a serious threat [1]. In this crime, a criminal uses your personal data (such as your social security number, address, and credit card accounts) to assume your identity, opening credit cards or bank accounts in your name.

Another important privacy issue is the right of employers to monitor the telephone, e-mail, and other communications of their employees or to use video cameras to monitor their employees. With inexpensive web cameras, even a home computer user may be tempted to monitor a babysitter or a cleaning person while away from home. Is this legal or ethical? Legislators and ethicists are still struggling with these complicated issues.

In the sphere of e-commerce, companies now collect an enormous amount of data (so-called "big data") about consumer purchases, interests, and buying patterns, using "cookies" and other advanced technology. Rules and laws lag behind such practices. Some consumers use anonymous web browsing to circumvent eavesdropping on their online activities, often with mixed results.

The Electronic Frontier Foundation, founded in 1990, has a long history of advocacy for privacy of Internet users. Their web site states:

> Above all, we need to respect the rights of autonomy, anonymity, association, and expression that privacy makes possible, while also taking into account legitimate law enforcement concerns. [1]

But it is not obvious at all why Internet users should have a right to privacy. An alternative would be to view the cyberspace as a public space. After all, drivers on public roads are not entitled to privacy: they are required to register and insure their cars and prominently display license plates and inspection stickers.

28.5.2 Censorship vs. Free Speech

In many societies, citizens are accustomed to enjoy great freedom of expression and the press. In the United States, these freedoms are defined as "fundamental rights" and protected by the First Amendment to the Constitution. There are limitations, though. Obscene speech, hate speech that incites to violence, and certain other forms of expression may be banned or restricted to adult audiences. These restrictions are much harder to control on the Internet because information is more readily accessible and minors are often the savviest computer users in the family.

Some have argued that technology, as it creates new ethical problems, also sometimes creates the means of solving them. For instance, filtering software can screen material on the Internet for certain types of words or images, automatically denying a user access to sites deemed obscene. However, software programs are not great judges of subjective human categories like obscenity. As an example, activists point out that word-screening filters can also block access to information about breast cancer. As usual, the promise of a technological "quick fix" is illusory.

A fairly recent debate can serve to illustrate these tough new questions. The debate is over whether public libraries should be required to ban access to pornographic web sites. In a 2003 ruling, the U.S. Supreme Court upheld a law that requires public libraries to install pornography filters on all computers with web access in order to continue receiving federal subsidies and grants. Interestingly, the American Library Association (ALA) argued against this decision. In its statement, the ALA said:

> "Libraries are a major information source in our society for access to the larger world of human expression. For some, they are the only available access point. Libraries connect individuals with the ideas, information, and images they seek. Libraries that raise barriers to access damage their credibility with their users.
>
> By providing information across the spectrum of human interests, and making them available and accessible to anyone who wants them, libraries allow individuals to exercise their First Amendment right to seek and receive all types of expression, from all points of view. Materials in any given library cover the spectrum of human experience and thought, even those that some people may consider false, offensive, or dangerous."

Yet in many states, minors are forbidden from unsupervised access to explicit sexual material in other settings (movies, magazines, etc.). Neither the Supreme Court's decision nor the ALA's objection is likely to end the debate on this issue.

A more recent controversy surrounds Google's and Yahoo's decisions for their operations in China to comply with the Chinese government's censorship laws prohibiting free political speech.

28.5.3 Intellectual Property and Copyright Issues

Another heated debate is raging over intellectual property rights, or, to put it plainly, the right of Internet users to copy and swap music files, videos, and books. The battle line is drawn between the recording industry and the young generation of Internet users who are used to getting their music for free on the web. The most celebrated early case was Napster, which was litigated out of existence in 2001. Aficionados of free music retaliated by embracing peer-to-peer (p2p) networks, which enable Internet users to locate and swap music and video files without a central repository.

Are such networks ethical? Are they legal? Again, there is no single answer to these tough questions. About the ethics there is serious disagreement. The recording industry argues that recording artists, producers, and engineers should get fair compensation for their hard work. Music fans claim that music sharing on the Internet actually promotes music, helps less known artists, and ultimately increases sales. After all, they argue, if you set up a shelf for swapping books, no one will find it illegal or unethical. Many youth hostels and vacation spots have such take-a-book-leave-a-book shelves. More people get involved in reading and eventually buy the books they liked. For many young people, the Internet offers such a swap center for music.

From a legal prospective, it is clear that copyright laws protect intellectual property such as books, music, videos, and computer software [1]. Recently, the recording industry has taken larger p2p software providers and individuals to court and claimed some victories. But enforcement alone cannot stop people from getting around the law. For example, music swapping web sites can be set up overseas in countries that have not joined the international convention on copyright protection. Because the industry must rely on the good will of its customers, conflicts like this will eventually be resolved through some market-demanded compromise. The music companies cannot afford to alienate their best customers, and music lovers cannot afford to keep breaking the law. New technologies and service models have emerged to meet the demand, such as a pay-per-song model.

In the area of software licensing, approaches range from lengthy incomprehensible user agreements written by lawyers to open source software. Individual software users often check the required box to accept a user agreement without reading — they don't have much choice. Open source software [1, 2] has gained much influence in the last decade and has saved money to individual consumers and big and small companies.
One major advance in the intellectual property debate is the Creative Commons initiative. According to the Creative Commons web site [1], "Creative Commons is a nonprofit organization that helps overcome legal obstacles to the sharing of knowledge and creativity to address the world's pressing challenges." Creative Commons has defined several standard licenses that define the terms for using your intellectual property. The licenses have simple diagrams and brief summaries written in plain English. An author can choose any one of these licenses for managing rights to his or her original work. For example, the CC BY-NC-SA license allows users to distribute, remix, adapt, and build upon the material in any medium or format for noncommercial purposes only, and only so long as attribution is given to the creator. If you remix, adapt, or build upon the material, you must license the modified material under identical terms. Creative Commons charges no fees, and no registration is required to use their web site.

Publishers, copyright holders, and hardware manufacturers have developed methods to limit distribution of information. These access control technologies are known as Digital Rights Management (DRM). A detailed description of DRM methods and techniques can be found on the Internet.

28.6 Summary

The evolution of computer and telecommunications technology and the ubiquitous use of computers is transforming our society in ways that could not have been anticipated even a few years ago and have brought on a host of social, ethical, and legal issues. The unprecedented rate of change gives little time to sociologists, ethicists and legal experts to reflect on and respond to the emerging technologies and their impact on society.

The best approach to all these issues may be the most general. The survival skills that bring success in school and in life — skills like critical thinking, problem solving, and moral reasoning — are also the best bet for handling the ethical quandaries that computers create. Certain character traits — empathy, adaptability, attention to detail — will help as well. And of course, a mastery of the technical details is almost essential. Used correctly, computers and the Internet can help you in acquiring this knowledge, character, and set of skills.

Suggested Activities

1. Which tools were used to create your school's web site? Was it created in-house or by an outside firm? Find out and report to your computer science class.

2. Locate the national statistics for drunk driving fatalities on the Century Council's web site [1]. Cut and paste the data from the PDF file presented on the site into Excel and print into a text file. While your teammate is preparing the data, write a Java application to find the period of five consecutive years with the lowest average mortality rate.

3. How many public schools with grades 9-12 are there in the U.S.? What is the average number of students per school? Find out by researching on the Internet.

4. Write a small GUI Java program that presents to its user a short online multiple-choice quiz. Create data files for several quizzes (for example, U.S. state capitals, English vocabulary words, definitions of object-oriented programming terms, and so on).

5. Create an account at codingbat.com [1] and, over a period of several weeks, solve at least 50 short Java programming problems there.

6. Explore the statistics for programming languages used on the Project Euler site [1]. While there, solve the first three problems [1]. Is Java or Python more convenient for solving such problems? Justify your answer.

7. Does your school or school district have an Acceptable Use Policy (AUP) document? Is it posted on the school's or district's intranet? (If not, find an AUP on another school's web site). Are there any provisions of the AUP that do you consider unnecessarily restrictive? Why? Discuss with your classmates.

8. Does your school use Google Drive, `dropbox.com`, or a similar service that allows students and teachers to conveniently share files? Or does your school have its own file sharing facility on its intranet? Investigate the pros and cons of using the school's intranet vs. an Internet service.

9. How does your own use of social networks compare with the U.S. averages? Do you agree that social networks should play a greater role in education? Why or why not? Discuss with your classmates.

10. Does your school allow smartphones and other mobile devices in the classroom? Do you support the school's policy on that matter? Do some of your teachers rely on mobile devices for teaching? Discuss with your teacher and classmates.

11. Have you ever had your personal computer infected with malware or ransomware? Do you know exactly when it happened? Discuss your experience with your classmates.

12. If a password must consist of 4 to 8 characters and can include digits and upper- and lowercase letters, how many such passwords exist? Approximately what percentage of all possible passwords are common English words in lowercase letters?

13. Do you use a password to log into your own personal computer? Why or why not?

14. Do you consider it OK to publish pictures of your friends on your social network page without their knowledge and permission? Why or why not?

15. Given a coding assignment, would you consider it ethical to start working on it by looking at examples of similar code on the web?

16. Search the Internet for images of phishing examples. Take a vote with your classmates on which one looks most authentic.

17. Describe the terms of the Creative Commons "Attribution-NonCommercial-NoDerivs 3.0 Unported" license. Is it a "free cultural work license"?

18. In March 2013, Google agreed to pay $7 million to 37 U.S. states to settle complaints that it violated people's privacy. What did Google do wrong? Research this incident on the Internet.

19. Suppose a book states on its copyright page that "No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise." If your teacher shows a page from that book on the screen in class, does he or she violate the publisher's copyright? Explain.

20. If you are a Facebook user, have you ever read the "Terms and Conditions" agreement? If you haven't, why not?

21. Name one or more recent social upheavals that have become known as "Twitter revolutions."

22. Name three or four uses of the Internet that, in your opinion, are bad for society.

23. Working in groups, research and present to the class a case of online bullying or "shaming" reported in the media, mentioning what happened and its consequences.

24. Research the "Do Not Track" Internet privacy initiative. Who is supporting it? Who is not and why?

25. What is *FinSpy*? Name a few governments that use it to spy on dissidents.

26. Find a definition of "VPN" and explain how it might be used.

27. Google researchers have pointed out "many familiar reasons why passwords don't cut it. Among them, that people choose them badly, lose them, write them down, and reuse them across services; that passwords can be intercepted by malware; and that password servers can be compromised over the Internet." What alternative technologies is Google experimenting with?

28. What is "steganography"? Research on the Internet and demonstrate its use to your classmates.

29. Read and discuss with your classmates Mat Honan's August 2012 column in the *Wired* magazine, "How Apple and Amazon Security Flaws Led to My Epic Hacking." Which security flaws led to Mat's problems? Is your "digital existence" vulnerable to similar threats?

30. What is "HONcode"? Why is it necessary? Which country hosts HON? How will your knowledge of HON change your web surfing practice?

31. In August 2012, a research team from Epic and the University of Oxford issued a preliminary report "Assessing the Accuracy and Quality of Wikipedia Entries Compared to Popular Online Encyclopaedias." Which online encyclopedias were used in comparison to Wikipedia in this research? What was the main conclusion of the report? Will you trust Wikipedia more or less as a result?

32. University of Maryland library has developed a guide for evaluating the quality and accuracy of information found on the web [1]. Discuss it with your peers. Does the UMD web site that hosts the guide meet its own high quality and accuracy criteria? Which items in the guide have you and your peers found most useful? Which of the items will you use in your future Internet research?

33. Name three main criticisms of DRM often brought up by free information exchange advocates and activists.