Cis1
Chapter 15
Computer Crime and Ethics
Book recommendation:

A Gift of Fire
Social, Legal, and Ethical
Issues in Computing

Sara Baase
Software Piracy
[illegal usage of software]

• The Industry group Business Software Alliance* (BSA) estimates piracy losses at $11.8 billion worldwide in 2000.
• 1 in 3 business software was pirated in 2000
• Worst offenders: Vietnam 97% China 94% Indonesia 89% (United States 24%)
• Individual consumers are not the problem

*includes Adobe, Apple, Autodesk, Macromedia, Microsoft and Symantec

Software and Information Industry Association
www.spa.org
Viruses

**Virus** - A software program that spreads from one computer to another computer in order to infect and corrupt other software files and data

May spread via files, disks, or over a network (email)

Viruses are not bugs, and are written on purpose.
Preventing Infection

Abstinence is the only 100% effective prevention method.

Anti-virus software - Programs designed to search for viruses, notify users when they are found, and remove them from infected files and disks. They can also monitor systems for suspicious activity, i.e. files being modified, disks being formatted, etc.

CERT- the Computer Emergency Response Team

www.cert.org  Information about viruses and Security vulnerabilities
Computer Crime

• Fraud and Embezzlement
• Sabotage and Information Theft
• Hacking and Cracking
• Digital Forgery

Software Piracy
Viruses
1. Fraud and Embezzlement

The most significant losses to businesses from computer crime come from employees.

Losses from credit card fraud are estimated to be between $1 and $4 billion per year.

ATM fraud accounts for losses of about $60 million a year.

Telecommunications fraud $1 to $9 billion each year.

Why? *Tradeoff between convenience and security*
2. Sabotage and Information Theft

Direct destruction of hardware, software or information

Use of “logic bombs”

An employee fired from an insurance company was convicted for destroying more than 160,000 records.

British Airways paid a competitor $4 million after hacking into their computers and stealing passenger lists.

Identity Theft (Information Collection, Privacy)
3. Hacking and Cracking

In the 1970’s John Draper discovered that the whistle in a cereal box could be used to fool the telephone system into giving free long-distance calls.

Clifford Stoll’s *The Cuckoo’s Egg* written about tracking a German hacker.

Kevin Mitnick, a notorious hacker, was arrested in 1995. He allegedly stole thousands of files from a computer security expert, credit card numbers, and unreleased software. (Book: *Takedown* by T. Shimomura)

High-Tech Low-Tech tricks:
Social Engineering, Shoulder Surfing, Dumpster Diving
4. Digital Forgery

Information accuracy?

Forgery and counterfeiting

Time magazine:  
*Darkening of O.J. Simpson’s skin*

National Geographic  
*Moved pyramids closer to fit on cover*

Solution:  
Be aware of the possibility  
Learn to have reasonable skepticism
Public Key Cryptography

*Let's you communicate with someone secretly without exchanging a code first.*

- Developed in 1972 by Diffie and Hellman
- Rivest, Shamir and Adleman (RSA) implemented it
- 1991 Philip Zimmerman developed a program (PGP) and gave it away for free – widely distributed over Internet – now most popular program for encryption in the world

*why? Put encryption in the hands of “the people”*
Can we trust Computers?

• Nationwide AT&T telephone service was disrupted for nine hours in 1990 because of a software error.
• U.S. Kane Carpet Company (4th largest) went out of business due to a bad computerized inventory control system
• Denver Airport computer-controlled luggage system helped keep the airport closed for 2 years – about $700 million lost
• The Therac-25 software-controlled radiation machine killed three and injured several in 1985-87

Why?
*Lack of testing, honesty, ethics*

“Perfection is not an option.”
Ethics

• Many schools report that plagiarism is on the rise
• (explicit copyright notices not required by international law)
• Computer Ethics Institute of the Brookings Institution – “Ten Commandments”
• ACM Code of Conduct
Ten Commandments Of Computer Ethics

1. Thou Shalt Not Use A Computer To Harm Other People.

2. Thou Shalt Not Interfere With Other People’s Computer Work.

3. Thou Shalt Not Snoop Around In Other People’s Computer Files.


5. Thou Shalt Not Use A Computer To Bear False Witness.

6. Thou Shalt Not Copy Or Use Proprietary Software For Which You have Not Paid.

7. Thou Shalt Not Use Other People’s Computer Resources Without Authorization Or Proper Compensation.

8. Thou Shalt Not Appropriate Other People’s Intellectual Output.

9. Thou Shalt Think About The Social Consequences Of The Program You Are Writing Or The System You Are Designing.

10. Thou Shalt Always Use A Computer In Ways That Insure Consideration And Respect For Your Fellow Humans.
The ACM Code of Conduct


As an ACM member I will ....

1.1 Contribute to society and human well-being.
1.2 Avoid harm to others.
1.3 Be honest and trustworthy.
1.4 Be fair and take action not to discriminate.
1.5 Honor property rights including copyrights and patent.
1.6 Give proper credit for intellectual property.
1.7 Respect the privacy of others.
1.8 Honor confidentiality.
For more information…

• Electronic Frontier Foundation
  www.eff.org
  Protecting Rights and Promoting Freedom on the Electronic Frontier

• Electronic Privacy Information Center
  www.epic.org

• The Association of Computing Machinery (ACM)
  www.acm.org

• Computer Professionals for Social Responsibility
  www.cpsr.org
  A public-interest alliance of computer scientists and others concerned about the impact of computer technology on society