This course is not primarily a lecture course. It will rely heavily on a discussion of the issues presented in the textbook *Computer Ethics: A Global Perspective* by Giannis Stamatellos. These slides present ideas and quotes from the textbook primarily to inspire and promote discussions in class. A focus will be placed on 1) the local and global impact of computing on organizations and society as well as on 2) how ethical principles and leadership quality impact individuals, organizations and society.
Method of enquiry of the textbook.

• Name of the issue? (e.g., computer crime)
• IT developments that refer to the issue? (e.g. database, internet)
• Part of information society affected? (e.g., online banking)
• Who is affected? (e.g., individuals, groups, organizations)
• Who is responsible/accountable? (e.g., sw developers, managers)
• Solutions to the problem? (e.g., legislations, policies, standards, maintenance)
computer crime

“any illegal act for which knowledge of computer technology is used to commit the offense” (National Institute of Justice)

“any criminal act that has been committed using a computer as the principle tool” (Forester and Morrison)

“illegal activities in which a computer is involved either as an object, subject, or instrument of the criminal act”
Computer crimes

1. Transformations of old crimes: theft, fraud, sabotage, espionage

2. New types of crime: unauthorized access into computer networks, cyberterrorism, computer sabotage
“... most analysts believe that the actual amount of computer crime is much greater than reported.”

Two reasons:

1. Difficult to detect in some cases.
2. Company cover-ups to protect public image.
Ch. 2 - Computer Crime and Security

computer criminals:

1. insiders – persons who work for the company or organization when the crime occurred

2. outsiders – persons who have no direct relationship with the place where the crime occurred (e.g., hackers, terrorist groups)
Ch. 2 - Computer Crime and Security

computer criminal motivations:

• wish to gain money or goods
• enjoy the challenge of breaking into a system
• to sabotage persons or machines
• to take revenge for personal reasons
• to perform acts of terrorism
• to spread political viewpoints
• etc.
Ch. 2 - Computer Crime and Security

Two basic categories of computer crime (Edgar):

1. Crimes against computers.
   a. Damage to hardware.
   b. Damage to software.

2. Crimes committed using computers.
   a. Theft of funds - embezzlement.
   b. Theft of services.
   c. Theft of information.
   d. Theft of goods.
   e. Counterfeiting.
   f. Organized computer crime.
Ch. 2 - Computer Crime and Security

**computer fraud**

“... any technique aimed at manipulating information within a computer system for the purpose of illicit (usually financial) gain.”

Like other computer crimes computer fraud can be

1. Computer-related fraud

2. Computer-assisted fraud – the computer is used actively to commit the fraud.
Computer fraud can be theft of

1. Money (e.g., unauthorized transfer of funds)
2. Information (e.g., unauthorized entry into a database)
3. Goods (e.g., redirect goods to other addresses)
4. Services (e.g., illegal use of cable TV channels)
Ch. 2 - Computer Crime and Security

Common types of computer fraud

1. ATM fraud – use of fake ATM card and the PIN
2. Electronic Fund Transfer (EFT) fraud – transfer of funds to private bank accounts
3. Electronic Data Interchange (EDI) fraud – steal information then use it or sell it
4. Credit card fraud
5. Telecommunication fraud – long-distance (illegal use of calling card codes) or mobile phone fraud
6. Cable TV fraud
7. Telemarketing fraud (redirection of goods or fake products sold
8. Internet stock fraud
hacking

“unauthorized access to computer material” (the Oxford Dictionary of Computing)

hacker (cracker):

“a person who attempts to breach the security of a computer system by access from a remote point, especially by guessing or otherwise obtaining a password” (the Oxford Dictionary of Computing)
Ch. 2 - Computer Crime and Security

Common hacking techniques that attempt to directly enter a system.

1. Piggybacking – use id and password of a legitimate user or login as a guest user

2. Scavenging/dumpster diving – look through discarded electronic data for information that would help entry into a system

3. Password guessing

4. Autodialing
Ch. 2 - Computer Crime and Security

Hackers can act

• directly - illegally entering a system themselves

• indirectly - embedding a destructive program in a system.
computer sabotage

Creation of small, destructive programs that cause serious hardware and/or software problems such as:

1. Deletion of files from disk.
2. Destabilizing the computer system.
3. Overloading email servers by sending emails to addresses on a victim’s address book.
4. Searching for and retrieving information about the person being hacked.
Types of programs used in computer sabotage:

1. viruses
   - “a self-replicating program reproduced by attaching executable copies of itself to other programs”
   - cannot run independently
   - requires a host program to infect and then is executed only when the host is run
   - spreads rapidly through hosts that share the same infected program or disk
Common types of viruses:

1. boot sector virus: infects system boot and is spread when the system is loaded.

2. email virus: is spread through email attachments

3. macro virus: is spread through documents that contain macros
Ch. 2 - Computer Crime and Security

2. worms

• “virus-like program that makes copies of itself across network connections, seeking uninfected workstations in which to reproduce.”

• travels independently through different sites

• more in the computer memory than on disk

• intent: reproductions cause memory or disk overload, system freeze, and loss of all data not previously saved

• a “memory virus” is removed by shutting down a system
3. trojan horse
   • destructive program made to seem like something useful or enjoyable (e.g., a game or utility)
   • may release other types of malicious software

4. logic bomb – secret destructive program that executes when a certain event occurs

5. time bomb – secret destructive program that executes when a particular time-related event occurs

6. spyware – surveillance software
Ch. 2 - Computer Crime and Security

Approaches to preventing computer crime.

1. Computer security and management
   a. “... protection of hardware, software, machines and networks from unauthorized break-ins, e-attacks, misuses and malfunctions.“
   b. Security breaches can affect
      a. The reliability and integrity of data.
      b. The confidence of the public in a business or organization.
Ch. 2 - Computer Crime and Security

1. Computer security and management (continued)

   c. **Common ways to maintain security:**
      
      I. Restrictions on physical and digital access.
      
      II. Backup of data.
      
      III. Encryption of stored data.
      
      IV. Encryption of data transmissions.
      
      V. Firewalls and anti-virus programs to stop unauthorized access.
      
      VI. Authentication schemes (e.g., dial-back systems, biometrics).
Ch. 2 - Computer Crime and Security

1. Computer security and management (continued)

   d. Authentication is a major problem for commercial and government business as well as national security.
      (Note: biometrics – digitizing the biological characteristics of a person (blood vessel patterns in the iris or backs of hands, fingerprints, voice, etc.)

   e. **Components of a complete security system.**

      d. Well designed authority and security levels.

         I. User-friendly security procedures.

         II. Use of security codes and passwords.

         III. Monitoring of suspicious internal/external activity.
Ch. 2 - Computer Crime and Security

Approaches to preventing computer crime:

2. Creation of legislation, policies, standards
   a. In 1986 the main federal computer crime law for computers and telecommunications was passed – *Computer Fraud and Abuse Act*
   b. This act is used by government agencies like the Federal Trade Commission (FTC) and the Securities Exchange Commission (SEC) to search network databases for illegal or suspicious activities and postings.

3. Education and “moral awareness”
Ch. 2 – Study Guide

• Define computer crime.

• Define the following types of computer crime: computer fraud, hacking, computer sabotage.

• Name several common types of computer fraud.

• Describe three common hacking techniques.

• What types of programs are commonly used in computer sabotage?

• Describe three approaches to preventing computer crime.

• Explain what is meant by computer criminals that are insiders/outsiders.

• What are the two basic categories of computer crime?
Ch. 2 – Study Guide

In the questions below the phrase *computer crime* could be replaced by a specific type of computer crime.

- Give an example of the local impact of *computer crime*.
- Give an example of the global impact of *computer crime*.
- Give an example of ethical principles related to *computer crime* and their application in leadership. For example, in what context (education, government, business, etc.) might leadership be effective in preventing or stopping computer crime?
- Give an example of the legal dimensions of *computer crime*. For example, consider traditional crime analogs, transformed types of crime, new types of computer crime.
- What major legislation is used to deal with computer crime and which government agencies are using that legislation?
- How does the ACM professional code address *computer crime*?
Ch. 2 – Study Guide

- Name several common ways that security is maintained in computer systems.
- Name the main components of a complete security system.
- Name three approaches to preventing computer crime.
- Give an example of the local impact of security issues related to computers and/or telecommunications.
- Give an example of the global impact of security issues related to computers and/or telecommunications.
- Give an example of ethical principles related to the security of computers and networks and their application in leadership. For example, in what context (education, government, business, etc.) might leadership be effective in supporting and improving the security of computer and network systems?
- How does the ACM professional code address computer and network security?