Computer Security (SCSR 3413)
Tutorial 1

---

1. Define computer security.
2. What is the OSI security architecture?
3. What is the difference between passive and active security threat?
4. List and briefly define categories of passive and active network security attacks.
5. List and briefly define categories of security services.
6. List and briefly define categories of security mechanisms.
7. Consider an automated teller machine (ATM) in which users provide a personal identification number (PIN) and a card for amount access. Give examples of confidentiality, integrity and availability requirement associated with the system and in each indicate the degree of importance of the requirement.
8. Consider a desktop publishing systems used to produce documents for various organizations.
    a. Give an example of a type of publication for which confidentiality of the stored data is the most important requirement.
    b. Give an example of a type of publication in which data integrity is the most important requirement.
    c. Give an example in which system availability is the most important requirement.

9. For each of the following assets, assigns a low, medium, or high impact level for the lost of confidentiality, availability and integrity. Justify your answers.
    a. An organization managing public information on its Web server
    b. A law enforcement organization managing extremely sensitive investigative information.
    c. A financial organization managing routine administrative information (not privacy-related information).
    d. An information system used for large acquisitions in contracting organization contains both sensitive, pre-solicitation phase contract information and routine administrative information. Assess the impact for the two data sets separately and the information system as a whole.
    e. A power plant contains a SCADA (supervisory control and data acquisition) system controlling the distribution of electric power for large military installation. The SCADA system contains both real-time sensor data and routine administrative information. Assess the impact for the two data sets separately and the information system as a whole.

10. Classify each of the following as a violation of confidentiality, of integrity, of availability, or of some combination thereof.
    a. John copies Mary's homework.
    b. Paul crashes Linda's system.
    c. Carol changes the amount of Angelo's check from $100 to $1,000.
    d. Gina forges Roger's signature on a deed.
    e. Rhonda registers the domain name "AddisonWesley.com" and refuses to let the publishing house buy or use that domain name.
    f. Jonah obtains Peter's credit card number and has the credit card company cancel the card and replace it with another card bearing a different account number.
    g. Henry spoofs Julie's IP address to gain access to her computer.

11. Identify mechanisms for implementing the following. State what policy or policies they might be enforcing.
    a. A password-changing program will reject passwords that are less than five characters long or that are found in the dictionary.
    b. Only students in a computer science class will be given accounts on the department's computer system.
    c. The login program will disallow logins of any students who enter their passwords incorrectly three times.
    d. The permissions of the file containing Carol's homework will prevent Robert from cheating and copying it.
    e. When World Wide Web traffic climbs to more than 80% of the network's capacity, systems will disallow any further communications to or from Web servers.
    f. Annie, a systems analyst, will be able to detect a student using a program to scan her system for vulnerabilities.
    g. A program used to submit homework will turn itself off just after the due date.

12. Give an example of a situation in which a compromise of confidentiality leads to a compromise in integrity.

13. Show that the three security services—confidentiality, integrity, and availability—are sufficient to deal with the threats of disclosure, disruption, deception, and usurpation.

14. For each of the following statements, give an example of a situation in which the statement is true.
    a. Prevention is more important than detection and recovery.
    b. Detection is more important than prevention and recovery.
    c. Recovery is more important than prevention and detection.

15. Computer viruses are programs that, among other actions, can delete files without a user's permission. A U.S. legislator wrote a law banning the deletion of any files from computer disks. What was the problem with this law from a computer security point of view? Specifically, state which security service would have been affected if the law had been passed.

16. Users often bring in programs or download programs from the Internet. Give an example of a site for which the benefits of allowing users to do this outweigh the dangers. Then give an example of a site for which the dangers of allowing users to do this outweigh the benefits.

17. An organization makes each lead system administrator responsible for the security of the system he or she runs. However, the management determines what programs are to be on the system and how they are to be configured.
    a. Describe the security problem(s) that this division of power would create.
    b. How would you fix them?

18. A graduate student accidentally releases a program that spreads from computer system to computer system. It deletes no files but requires much time to implement the necessary defences. The graduate student is convicted. Despite demands that he be sent to prison for the maximum time possible (to make an example of him), the judge sentences him to pay a fine and perform community service. What factors do you believe caused the judge to hand down the sentence he did? What would you have done were you the judge, and what extra information would you have needed to make your decision?