1.12. Exercises

1: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.

2: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.

3:The aphorism “security through obscurity” suggests that hiding information provides some level of security. Give an example of a situation in which hiding

information does not add appreciably to the security of a system. Then give an example of a situation in which it does.

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

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

6: In addition to mathematical and informal statements of policy, policies can be implicit (not stated). Why might this be done? Might it occur with informally stated policies? What problems can this cause?

7: 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.

8: Is it possible to design and implement a system in which **no** assumptions about trust are made? Why or why not?

9: Policy restricts the use of electronic mail on a particular system to faculty and staff. Students cannot send or receive electronic mail on that host. Classify the following mechanisms as secure, precise, or broad.

a. The electronic mail sending and receiving programs are disabled.

b. As each letter is sent or received, the system looks up the sender (or recipient) in a database. If that party is listed as faculty or staff, the mail is processed. Otherwise, it is rejected. (Assume that the database entries are correct.)

c. The electronic mail sending programs ask the user if he or she is a student. If so, the mail is refused. The electronic mail receiving programs are disabled.

10: Consider a very high-assurance system developed for the military. The system has a set of specifications, and both the design and implementation have been proven to satisfy the specifications. What questions should school administrators ask when deciding whether to purchase such a system for their school's use?

11: How do laws protecting privacy impact the ability of system administrators to monitor user activity?

12: 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.

13: 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.

13

14: A respected computer scientist has said that no computer can ever be made perfectly secure. Why might she have said this?

15: 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?

16,18,19,20,21

16: The president of a large software development company has become concerned about competitors learning proprietary information. He is determined to stop them. Part of his security mechanism is to require all employees to report any contact with employees of the company's competitors, even if it is purely social. Do you believe this will have the desired effect? Why or why not?

17: The police and the public defender share a computer. What security problems does this present? Do you feel it is a reasonable cost-saving measure to have all public agencies share the same (set of) computers?

18: Companies usually restrict the use of electronic mail to company business but do allow minimal use for personal reasons.

a. How might a company detect excessive personal use of electronic mail, other than by reading it? (**Hint**: Think about the personal use of a company telephone.)

b. Intuitively, it seems reasonable to ban **all** personal use of electronic mail on company computers. Explain why most companies do not do this.

19: Argue for or against the following proposition. Ciphers that the government cannot cryptanalyze should be outlawed. How would your argument change if such ciphers could be used provided that the users registered the keys with the government?

20: For many years, industries and financial institutions hired people who broke into their systems once those people were released from prison. Now, such a conviction tends to prevent such people from being hired. Why you think attitudes on this issue changed? Do you think they changed for the better or for the worse?

21: 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 defenses. 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?

19)I agree with the proposition that there should not exist ciphers that the government cannot cryp analyze because those ciphers could be used to obscure dangerous behaviors such as child pornography from law enforcement – which has been gi... view the full answer