Answers to Selected Chapter 1 Exercises

Note: Student answers, and your answers, to any of these questions may vary from the answers here. That's okay, because one looks at these questions with a particular environment in mind (in other words, we make assumptions). The key issue is whether the answer the student, or you, give can be justified. The acceptability of the answer depends upon the quality of the justification.

1.
   a. John copying Mary's homework is a violation of confidentiality. John should not see Mary's homework because to copy homework is cheating.
   b. Paul crashing Linda's system is a violation of availability. Linda's system is no longer available to her, or anyone else.
   c. Carol changing the amount of Angelo's check from $100 to $1000 is a violation of integrity (specifically, data integrity). The amount written on the check has been changed.
   d. Gina forging Roger's signature on a deed is a violation of integrity (specifically, integrity of origin). The deed appears to have come from Roger, when in fact it came from Gina.
   e. Rhonda registering the domain name "AddisonWesley.com" and refusing to let the publishing house buy or use that domain name is a violation of availability. The name "Addison-Wesley" is not available to anyone, including the owner of that name, except Rhonda.
   f. Jonah obtaining Peter's credit card number, and having the credit card company cancel the card and replace it with another bearing a different account, is a violation of integrity (specifically, integrity of origin). The request appears to come from Peter (else the credit card company would not have honored it), but in reality came from Jonah.
   g. Henry spoofing Julie's IP address to gain access to her computer is a violation of integrity (specifically, integrity of origin). The messages from Henry appear to come from Julie's IP address, when in fact they do not.
2.
   a. The policy element is that easily guessed passwords are forbidden. The mechanism element is the program checking for, and rejecting, those passwords.
   b. The policy element is that only students in that class may use the department's computer system. The mechanism element is the procedure of not giving other students an account.
   c. The policy element is that only authorized users may log in. The mechanism element is that after three failed login attempts, the system disables the account to prevent further guessing of the password
   d. The policy element is that no student may read another student's homework. The mechanism element is the file protection mechanism that restricts read access.
   e. The policy element is that World Wide Web traffic may not interfere with other network traffic, such interference being defined as using more than 80% of the bandwidth. The mechanism element is to block any traffic to or from Web servers.
   f. The policy element is that systems may not be scanned for vulnerabilities. The mechanism element is whatever Annie used to detect the scanning.
   g. The policy element is that late homework is not accepted. The mechanism element is the program disabling itself after the due date.
3. An example of a situation in which hiding information does not add appreciably to the security of a system is hiding the implementation of the UNIX password hashing algorithm. The

algorithm can be determined by extracting the object code of the relevant library routine and disassembling it. (The library must be world readable in order for user programs to load the routine.) Revealing the algorithm does not appeciably simplify the task of an attacker because he knows how to hash passwords, but he still must guess the password itself.

An example of a situation in which hiding information adds appreciably to the security of a system is hiding a password or cryptographic key. This is a private piece of information affecting only a single user. Revealing it would give an attacker immediate access to the system.

4. If the confidentiality of a password is compromised, the attacker may be able to impersonate a user authorized to change data. As integrity requires that only authorized users make only authorized changes to data, and the attacker is not an authorized user, there is a violation of integrity..
5. Disclosure is the revealing of information, so the confidentiality security service is sufficient to deal with that threat. Disruption is the interruption or prevention of a service. The security service of availability counters interruption, and ensures the service can be supplied, countering prevention also. Deception is the acceptance of false data. The data may be the contents of something, or the origin of something. The security service of integrity handles both of these. Usurpation is the unauthorized control of a service. The security service of integrity prevents an unauthorized user from altering the origin of the control of the service; the security service of availability ensures the authorized controller an still control the service.
6. Policies may be implicit for a number of reasons. The policy may be ambiguous, and the resolution of the ambiguity left to the reader; thus, the exact policy is not explicitly stated. The policy may not cover all aspects of the system; those aspects not covered by the explicit policy would presumably be covered by the implicit policy. The institution owning the computer may simply choose to tell users to use “common sense”; this is also an implicit policy. It is highly likely that informally stated policies will have many areas of ambiguity and not cover all contingencies. Hence these types of policies often lead to implicit policy components.

   The main problem with implicit policies is that not all users may know about them, or may have agreed to them. The statement that “common sense is so unusual because it’s not common” applies here. Given that people cannot refer to an oracle, or source, for an implicit policy but insteadmust gather opinions and make their own decisions, which may disagree with those of the system managers, a user may find herself violating the security policy without realizing it or intending to violate it.
7.
   a. An example of when prevention is more important than detection and recovery is the nuclear command and control system. By the time an intrusion is detected and recovered from, an attacker could have launched nuclear weapons.
   b. An example of when detection is more important than prevention and recovery is in the protection of medical records from unauthorized emergency room personnel. If someone is brought into an emergency room, there may not be time to secure the patient’s permission to access his medical records. But if the records are accessed illicitly, the security personnel should detect it.
   c. An example of when recovery is more important than prevention and detection is on a banking computer that maintains account balances. The bank must be able to recover the balance of all accounts to ensure it provides accurate service to its customers. Prevention and detection, while important, are not so important as keeping the balances accurate.

8. It is not possible to design and implement a system in which *no* assumptions about trust are made. Designing and implementing any system involves people, and the people must be trusted to design and implement the system correctly. If one does not trust the people, their work must be checked, and the people doing the checking must be trusted. Iterating this lack of trust demonstrates that some people doing checking must be trusted, unless the checking is automated. But in that case, people implemented the automated checker. This is equivalent to the previous case.
9.
    a. The mechanism is secure, because students cannot send or receive electronic mail on the system. It is not precise, as faculty cannot send or receive electronic mail on the system, and the security policy says they are allowed to.
    b. This mechanism is precise, because any mail from or to students is discarded. (You can argue this is broad, because students can execute the "send mail" command, but the mail will never leave the machine. The word "send" is somewhat ambiguous.)
    c. This mechanism is broad, because a student can claim to be a faculty member when answering the question.
10. Some example questions follow.
    a. Are the specifications appropriate for an educational institution? For example, will the military system meet the availability needs of the university?
    b. What assumptions about the operating environment does the military system make? Are the assumptions valid in the school's operating environment?
    c. What procedures must be followed to record and distribute grades? Does the system specification assure this can be done in a way that meets the requirements of the university?
11. Laws protecting privacy forbid the collection of some types of data. The goal of these laws is to prevent an organization, or individuals, from inferring information about individuals' beliefs, behavior, or other personal characteristics from the data being transmitted. When monitoring user activity, privacy laws affect system administrators because they cannot observe certain data relating to user activity. For example, a user may read private e-mail from her spouse. The contents of that e-mail, if protected by privacy laws, must be suppressed when the system administrator records network traffic. So the system administrators must devise a method to conceal or scramble the information (called *sanitization*). The problem becomes more complex when the information is relevant to a security analysis. For example, consider a sweep of a network looking for HTTP servers. That this is a sweep will be obvious when the IP addresses are correlated: every IP address on the network will have been probed. But the IP addresses may tie machine use to an individual user, so a law restricting the ability of the system administrator to tie actions to specific users may prevent the recording of the IP addresses. This would hinder the security analysis of the user activity, because some of those activities could not be recorded.
12. The problem with the proposed law was that *any* deletion was forbidden. As written, if someone dragged a file to the trash can or recycle bin (or otherwise deleted the file), that person would violate the law. Further, not all viruses delete files. Some transmit information; others insert back doors (indeed, Cohen's early viruses were of this type). So the law would not achieve its desired purpose, and indeed would criminalize acts that have nothing to do with computer viruses. The specific security services that could be affected by this law would be

availability (if you can't delete files, you will run out of room on the disk) and integrity (the system may require that certain files be deleted to function correctly).

13. An example of a site at which the benefits of allowing users to download programs outweigh the dangers would be a university. Much of the free software that universities depend on, such as the text editor *emacs*, must be downloaded. Without these free programs, students would not be exposed to such a wide variety of software and systems, and this would adversely affect their education. Further, the students rarely have the privilege to alter system programs, so they can damage only their protection domain if they download malicious code.
    An example of a site at which the dangers of allowing users to download programs outweigh the benerfits would be a site at which sensitive data is handled, such as a medical insurance company (patient medical records) or a classified facility. The problem is that the downloaded code could transmit, alter, or delete data, and the data is very sensitive to exposure or unauthorized alteration. If damaged, reconstructing the data would be very expensive (if the data could be reconstructed); if made public, the damage could not be undone.
14. When the respected computer scientist said that no computer can ever be made perfectly secure, she was probably thinking about the people who use it. No matter how secure the system, some of the users, administrators, and programmers have access to information on the system, and the ability to alter the system programs. (Two or more people may need to work together for this purpose.) The human element here is the weak point, because people can be corrupted or threatened, or otherwise persuaded to breach system security.
15.
    a. The division of power gave the system administrators the responsibility for securing the systems, but denied them the power to determine what programs could be run and how the systems were to be configured. Responsibility without power is untenable because the matter for which one bears responsibility is notunder one's control. So, the system administrators were (essentially) scapegoats.
    b. The best way to fix the problem is to allow the system administrators to determine what programs could be run and how their systems would be configured. So, the managers (and system administrators) would together set a reasonable policy, and then the job of the system administrators would be to ensure their systems (and their system interactions) conform to the policy. This way, the management goals with respect to "security" are clearly stated, and the system administrators are given both the power and the responsibility for ensuring the policy is met on the actual systems.
16. The president's edict raises several issues.
    First, will it solve the problem? If the employees are not involved, the measure will not help the situation, and could make matters worse (see below). If the employees are involved, presumably not all of them are involved, so measures that would be effective against the culprits should be taken. If it is not known whether any employees are involved, the intent of this method seems to be that, if the leaks stop, then the employees are leaking the information. But the leaks stopping could also be due to the leaker becoming nervous and deciding to lay low while the ban is in effect, or for a variety of reasons unrelated to the ban. A more precise method of determining *which* employees, if any, were leaking should be used.
    Second, how will the employees feel about it? If the employees understand the reason for the measure, and accept it, there will be no problem. But some employees may feel that the need to report even social contacts is an infringement on their personal lives. These people may resent the edict, and may not comply. Even those who comply may resent the intrusion into

their personal lives. Such a situation would be disastrous for employee morale, and may lead to more problems than the leak of proprietary information.

This raises a critical point: how can the president enforce his rule? Consider the case of a corrupt employee who has a role in competitors learning proprietary information. How likely is that employee to report his or her contacts with the competitor's employees? Unless the president has a way of validating that all contacts are indeed reported, the result of the measure seems to be that the honest employees will comply and the dishonest ones will not—achieving exactly the opposite of the goal of the edict.

So, whether this measure has the desired effect depends on three factors. First, if the president can verify that no contacts other than those reported have occurred, then the measure would show which employees are talking to people from the competitors. Second, if the president can establish that information s leaking through contacts such as those, then the president will know which subset of employees have to be watched. But both of these hypotheticals are highly unlikely, for the reasons given above. Further, the edict could hurt morale severely, leading to a loss of productivity and of key people.

17. Not answered here.
18.
    a. Companies can detect excessive personal use of a telephone by looking at the numbers dialed. If those numbers belong to people not related to, or involved in, the company's business, the company may investigate further to determine if the employee is using the phone for too much personal business. Similarly, with electronic mail, the company can note the outgoing addresses, and from those determine if the employee is using email for personal business. These methods are typically cumbersome and require investigation, so they tend not to be used unless phone calls or email is severly affecting the budget of the organization or the productivity of the employees.
    b. Banning all personal use of electronic mail might significantly decrease the time employees spend working. Should a personal call need to be made (or received), the employee would have to find a phone not belonging to the employer. This could take considerably more time than simply making the call from the employee's phone (for example, if the employee has to go out of the building and across the street to a drug store or gas station). An additional factor is employee morale; knowing that the employer does not trust employees enough to control their personal calls can hurt morale.
19. Not answered here.
20. Not answered here.
21. Not answered here.