به نام خدا

تمرین های فصل اول

مرضیه علیدادی 9631983 – مریم السادات ثمره هاشمی 9724883

---

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.

Confidentiality. John should not see Mary's homework because to copy homework is cheating.

   b) Paul crashes Linda's system.

Availability. Linda's system is no longer available to her, or anyone else.

   c) Carol changes the amount of Angelo's check from $100 to $1000.

Integrity. The amount written on the check has been changed.

   d) Gina forges Roger's signature on a deed.

Integrity. The deed appears to have come from Roger, when in fact it came from Gina.

   e) Rhonda registers the domain name "AddisonWesley.com" and refuses to let the publishing house buy or use that domain name.

Availability. The name "Addison-Wesley" is not available to anyone, including the owner of that name, except Rhonda.

   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.

integrity. The request appears to come from Peter, but in reality came from Jonah.

g) Henry spoofs Julie's IP address to gain access to her computer.

Confidentiality, integrity. The messages from Henry appear to come from Julie's IP address, when in fact they do not

---

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.

Authentication. The policy element is that easily guessed passwords are forbidden. The mechanism element is the program checking for, and rejecting, those passwords.

b) Only students in a Computer science class will be given accounts on the department's computer system.

Access control. 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 login program will disallow logins of any students who enter their passwords incorrectly 3 times.

Authentication. 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 permissions of the file containing Carol's homework will prevent Robert from cheating and copying it.

Confidentiality, authentication. 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) When World Wide Web traffic climbs to over 80% of the network's capacity, systems will disallow any further communications to or from Web servers.

Monitor and response. 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) Annie, a system analyst, will be able to detect a student using a program to scan her system for vulnerabilities.

Monitor and response. The policy element is that systems may not be scanned for vulnerabilities. The mechanism element is whatever Annie used to detect the scanning.

g) A program used to submit homework will turn itself off just after the due date.

The policy element is that late homework is not accepted. The mechanism element is the program disabling itself 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.

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.

---

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.

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) Detection is more important than prevention and recovery.

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) Recovery is more important than prevention and detection.

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

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. 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.

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) 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.)

This mechanism is precise, because any mail from or to students is discarded.

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.

This mechanism is broad, because a student can claim to be a faculty member when answering the question.

---

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

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. 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.

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, that person would violate the law. Further, not all viruses delete files. Some transmit information; others insert back doors. 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).

---

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

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.

---

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

A public defender is a public attorney who represents people charged with a crime but who cannot afford to hire a private attorney. The defender's interests in protecting his client may be different from those of the police leading to a conflict of interest, and a confidentiality violation. Sharing access to resources among entities with a potential conflict-of-interest is a security threat.