IS-2150/TEL-2810 Introduction to Security

Homework 1
Due Date: September 13, 2007
Total: 50 Points

1. [36 Points] Do the following from Chapter 1

From section 1.11, do exercises 1, 5, 7, 9, 12, 15 (6 points each)

Exercise 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**]
b. Paul crashes Linda's system. [**availability, integrity**]
c. Carol changes the amount of Angelo's check from $100 to $1,000. [**data integrity**]
d. Gina forges Roger's signature on a deed. [**integrity**]
e. Rhonda registers the domain name "AddisonWesley.com" and refuses to let the publishing house buy or use that domain name. [**availability**]
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. [**confidentiality, integrity, availability**]
g. Henry spoofs Julie's IP address to gain access to her computer. [**source integrity**]

Exercise 5: Show that the three security services—confidentiality, integrity, and availability—are sufficient to deal with the threats of disclosure, disruption, deception, and usurpation. (solution is previous submission)

Unauthorized access to information is *disclosure*. For instance, snooping which is the unauthorized interception of information, is a form of disclosure. *Confidentiality* services counter this threat.

Acceptance of false data is called *deception*. For instance, the man-in-the-middle attack is a kind of deception, where the receiver and sender do not realize that an intruder is reading the sent information and possibly sending false information to the receiver. *Integrity* services counter this threat.

Interruption or prevention of correct operation is called *disruption*. Denial of service is an instance of disruption. The attacker may prevent the server from providing service to the requesting client. *Availability* services take care of this threat.

Unauthorized control of some part of the system is called *usurpation*. Masquerading or pretending to be someone else to control a system is a kind of usurpation. *Integrity* services (called "authentication services", in this context) counter this threat.

Therefore, three security services-confidentiality, integrity and availability- are sufficient to deal with the threats of disclosure, disruption, deception and usurpation.

Exercise 7: For each of the following statements, give an example of a situation in which the statement is true. (solution is previous submission)

a. **Prevention is more important than detection and recovery.**

Prevention of virus Infection in a computer is more important than its detection and recovery. If a computer is already infected with a virus, it may corrupt and delete data, which may not be recoverable.

b. **Detection is more important than prevention and recovery.**

Prevention of virus Infection in a computer is more important than its detection and recovery. If a computer is already infected with a virus, it may corrupt and delete data, which may not be recoverable.

c. **Recovery is more important than prevention and detection.**

In a hard disk crash, recovery of the users files and other information is more important. All Hard disks are probable to crash after some time, so it is hard to prevent such crashes, but a recovery plan should be put in force before hand by using RAID arrays and weekly backups.

Exercise 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.

[**secure**]

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.)

[**precise**]

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.

[broad]

Exercise 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.

Confidentiality: In case of successful attack on the system, loss of private data may occur.
Integrity: Malfeasant executables could cause source and data integrity.
Availability: Loss of storage space can eventually lead to availability problems.

Exercise 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. (solution is previous submission)

a. Describe the security problem(s) that this division of power would create.

Security mechanism in a company depends on who is responsible for the company's security. The power to implement appropriate controls must reside with those who are responsible. If management determines what programs are to be on the system, then the system administrators who are responsible for the security, who see the need for security measures will be unable to implement the appropriate security measures. Since management is not aware of the technical aspects of security as much as system administrators it's possible for management to make some poor choices with regard to cost, resources, security measures. Also coordination among the system coordinators is also pivotal in an organization and this coordination might be compromised if management makes the key security decisions.

b. How would you fix them?

The problem can be fixed by providing system administrators (knowledgeable people) with more control and sufficient resources for administering computer systems. Management should consult the system administrators before making any decision on security issues. If the company has several divisions each should have separate system administrator then the company can have one security head who is knowledge about security issues and who heads all the systems administrators. Management should leave all the key security decisions to him. Security head should take care of delegating the appropriate security tasks to the concerned system administrators. Part of the management role requires them to know about the cost, resources, security polices etc, and management can get up to date about these by consulting the security head.