Computer Security Chapter 1 Exercises

Mahya jamshidian

Fateme Rahmani

1 -

A- Confidentiality

B- Availability

C- Integrity

D- Integrity

E- Availability

F- Integrity , Availability

G- Integirity, Confidentiality

2-

A- policy is not using kown and weak passwords mechanism is a code to check for these passwords.

B- policy is other people don't have access to web site (authentication, integrity) and mechanism is to add them in the course by admin of class.

C- policy is prevention of the access of unauthorized students(access control), mechanism is to not allow to enter the site after three failed trial of password.

D- policy is prevent cheating(confidentiality), mechanism is to set permission of access of files.

E- policy is preventing from congestion in network, mechanism is to preventing making new connections until this situation.

F-

G- policy is preventing from late submisions, mechanism is set timeout for system.

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 Cryptography algorithm. The algorithm can be determined by extracting the object code from the relevant library routine. Revealing the algorithm does not appreciably simplify the task of an attacker because he still must guess the password itself.

However, hiding the cryptographic key, does add appreciably to the security of a system as its revealing will put users data in danger.

4-

For example if an attacker findes the admins passwords can change the files and make some fake data.

5-

- **Disclosure**: Confidentiality prevents disclosure.
- **Disruption**: Availability prevents Disruption.
- **Deception**: Integrity prevents accepting invalid data/entities.
- **Usurpation**: Availability and Integrity will prevent Usurpation.

6-

Some policies are very clear and sometimes we assume that this are accepted by everyone and they don't need to be said again in policies. This may make some problems for those how don't know these as obvious rules.

7-

1. 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.

2. Although prevention is always better than cure, Detection would be more important in cases when it is very hard to prevent a certain type of attack. This is true in Intrusion Detection Systems. For example, if a service is to be provided, there is always a threat of a Denial-of-Service attack. Such attacks should be detected first to prevent the unavailability of the service.

3. 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 .

8-

no it's not possible at least we must trust on some keys or mechanisms and assume that they wouldn't be broke.

9-

a. Secure
b. Precise
c. Broad

10-

A high assurance system that developed for military must cost too much that one school doesn't need because confidentiality in a school is not as important as military.

11-

Laws protecting privacy impact system administrators' ability to monitor user activity by requiring all parties assent to being recorded, in addition, if the sys admins' users are accessing the system remotely and they fall within different jurisdictions, then they may be committing a crime because of the different laws affecting user privacy in different jurisdictions (which may contradict each other).

12-

by using this method for avoiding a thread deleting files a normal user may have some problems using this system, and it violates 'availability' in system.

13-

When benefits outweigh the danger: Let's use checkpoints. If you download the toolbar, you get points which you can use for perks like giftcards and when you get enough points you can redeem them for something cool.

When danger outweighs the benefits: Let's use facebook. A user sees this offer on one of there favorite games. "$100 in facebook credit if you sign up and download our program." And they click on it and they sign up and download the program. You get the $100 dollars but they have a hidden virus that tracks your bank information and everypassword to every website that you are a member on.

14-

in computer security we trust some base rules and assume that they are not brokable but by passage of time they may be broke with new methods or computers that they wouldn't exist before.

15-

- The power to implement appropriate controls in a company 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.

- 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 Management should leave all the key security decisions to him. Part of the management role requires them to know about the cost, resources, security polices etc, management can get up to date about these by consulting the security head.

16-

I think it's not possible because he can't control all the meetings and check all of communication information and maybe a malicious employee wouldn't report the meeting and there is no mechanism to check if they report all meetings or not

17 -

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 dfferent from those of the police leading to a conflict of interest, and a confidentiality violation.

18-

all destination of mails that they are business mails are finite and they can make a list of business mails to determin personal usage
They may forgot to add some of the emails of work places, and ban all personal use of email decrease availability in the system that's not desirable.

19 -

For: If the government has backdoor access into the cipher system to be able to decrypt arbitrary messages, then stronger encryption systems (longer keys in typical marketing speak) can be used by the consumer.

Against: The government should not be able to inspect a person's encrypted transmissions without probable cause and a search warrant. Anything the government could cryptanalyze could also be analyzed by a malicious person either within the government or with the same resources.

20-

21-