Exercise 1

1. **Distinguish between vulnerability, threat, and control.**
   Vulnerabilities are weaknesses that can allow harm to occur. A threat is a set of circumstances that could cause harm. The control is a means to counter threats
2. **Theft usually results in some kind of harm. For example, if someone stealsyour car, you may suffer financial loss, inconvenience (by losing your mode oftransportation), and emotional upset (because of invasion of your personalproperty and space). List three kinds of harm a company might experience fromtheft of computer equipment.**
   The theft of computer results in data theft, and this data can be misused for unlawful activities. The work may be hampered, and the company need to arrange a backup system. The disturbed work environment may result in reduced work output, resulting financial losses. The lost information can result in business jeopardy. The PII information can result in financial loss too.
3. **List at least three kinds of harm a company could experience from electronicespionage or unauthorized viewing of confidential company materials.**
   The unauthorized viewing of confidential information can result in data breach, that can be used by competitors for causing damage to the company. The trade secrets, and business confidential information will be lost. The trust on the company may come down, thus resulting in financial losses. The reputation of the company is at stake, if critical information is viewed. This may result in increased threat to the rivals.
4. **List at least three kinds of damage a company could suffer when the integrityof a program or company data is compromised.**
   If the company data is compromised, then there is will threat to the organization, which results in physical,and financial damage to the company assets. The data can be misused, and used for wrong activities that results in harm to company's reputation. The data can be used in anti-social activities, or terrorist activities. E.g. the PHI data can be used to access individuals bank accounts, and credit cards, and misuse the funds. This data can be

used to create social networking accounts, and spread in appropriate content thus resulting in reputation damage to the company, and its clients. The data can be sold to terrorist organizations, and can be used for inappropriate activities.

5. **List at least three kinds of harm a company could encounter from loss ofservice, that is, failure of availability. List the product or capability to whichaccess is lost, and explain how this loss hurts the company.**

   The loss of service is the interruption to the service which can be a malicious, or non-malicious which can be accidental or intentional. The loss of service create frustration in the work environment, and hampers the work. The work delay results in delay in deliverable which can results in financial loss. The company's commitment to the delivery is at stake, and the confidence on future deliverable is questionable. The product can be software, or a hardware for which the access is lost. This result in work disturbance, and hampers the deliverables.

6. **Describe a situation in which you have experienced harm because of a failure of computer security. Was the failure malicious or not? Did the attacktarget you specifically or was it general and you were the unfortunate victim?**

   There was a situation in my work environment, in which the systems stopped working, and frequently handing in 15 minutes. This is a malicious activity, in which a program by passed the antivirus, and got installed in my network systems. This started running the background programs, thus resulted in using maximum ram, and thus abruptly shutting down. This attack in non-targeted attack, and generally affected all the systems. The program was uninstalled, and virus scan was done, and removed the extension files.

7. **Describe two examples of vulnerabilities in automobiles for which automanufacturers have instituted controls. Tell why you think these controls areeffective, somewhat effective, or ineffective.**

The automobile manufacturers are more worried about automobile hacking. The automobiles like cars can be accessed wirelessly, and can open the vehicle without authorization. The car speedometer can be manipulated, and programmed for maximum engine efficiency resulting in damage to the vehicle. Unauthorized applications, and malwares can be introduced in the vehicle, and can abruptly stop the engine resulting in accidents. The automobiles should be provided with controls to prevent automobile hackings.

8. **8. One control against accidental software deletion is to save all old versions ofa program. Of course, this control is prohibitively expensive in terms of cost ofstorage. Suggest a less costly control against accidental software deletion. Isyour control effective against all possible causes of software deletion? If not, what threats does it not cover?**

The backup is the best approach to prevent accidental deletion of software. The data can be taken back up in the hard drives, which are expensive. The clod backup is the best approach in taking secured backup with less cost. The infrastructure for cloud storage will not exponentially increases, unlike the hard disk which are costly, and storage require secured access. The cloud storage will be a third-party storage location, and need to rely on the third-party security control. Failure in third party cloud storage can result in data loss, unless they have efficient backup and recovery process.

9. **On your personal computer, who can install programs? Who can changeoperating system data? Who can replace portions of the operating system? Canany of these actions be performed remotely?**

The programs can be installed by system administrator only. No other person should make changes in the operating system data. The operating system can be changed using bootable disk. This can be performed by authorized, technical expert only. These can be performed remotely, but it is always suggested not to perform this activity remotely.

10. **Suppose a program to print paychecks secretly leaks a list of names of employeesearning more than a certain amount each month. What controls could be instituted tolimit the vulnerability of this leakage?**

The controls to limit the vulnerability is to remove the published data, to prevent further damage. The employees need to be trained to handle this kind of situation. The credit monitoring for the employees need to be conducted.

Chapter 2

1. Describe each of the following four kinds of access control mechanisms interms of (a) ease of determining authorized access during execution, (b) ease ofadding access for a new subject, (c) ease of deleting access by a subject, and (d)
ease of creating a new object to which all subjects by default have access.

•per-subject access control list (that is, one list for each subject tellsall the objects to which that subject has access)

•per-object access control list (that is, one list for each object tells allthe subjects who have access to that object)

•access control matrix

•capability

The per subject access control list

-The access of the subjects is determined for specific objects. The subjects are identified, and components to which the subjects need to be accessed are identified. The subject who requires access to the same objects can be easily addressed, and provided with same set of access permissions.

The per object access control list

- The determination of the access approval is simplified. The components that require access is determined and each subject's access is identified, and verified for approval. The addition of access to new subject is simplified. Another column can be easily embedded, with required authorizations. This will not impact the other subjects' authorizations.

Access control Matrix

- The approval is simple, because there is less number of items. If the subject needs to be added, or removed, then it will impact whole line, and the sections of the framework. This is made simple, by including a section in to the framework. This will be implemented to every subject.

Capability

- The approvals are simple in this, because the token will be added the the article according to solicitation. The subject can be provided with new operation that permits the actions on the object. The expansion, and cancellation of subjects is little confusing, and this includes changes in articles, and the obligations.

2. Suppose a per-subject access control list is used. Deleting an object in such asystem is inconvenient because all changes must be made to the control lists ofall subjects who did have access to the object. Suggest an alternative, less costlymeans of handling deletion.

Per object control run down can be implemented to resolve this issue. The rundown holds the information of every subject's accessible items. If the item is erases, or removed then the item is removed from the open articles of subject rundown.

3. File access control relates largely to the secrecy dimension of security. Whatis the relationship between an access control matrix and the integrity of theobjects to which access is being controlled?

The access control network contains subjects as lines, and questions as sections. The authorizations are defined as passages. The access control grid secures the articles trust, by providing access to known or defined clients. The sections ensure, that the items access by approved clients. The trustworthiness of the subject is protected, by preventing the unauthorized access to objects.

4. One feature of a capability-based protection system is the ability of oneprocess to transfer a copy of a capability to another process. Describe a situationin which one process should be able to transfer a capability to another.

-The capability is a ticket or kind of identification that provides access permission to the subjects, to access the specific objects. The capabilities are encrypted with a code or key to access the mechanism. The subject with capability of transfer a copy allows passing copies of capabilities to other subjects. The process A can pass copy of a capability to B. The B can pass acopy to C, but B will have a capability to restrict further distribution of capability by restricting the transfer capability to C. The capabilities are stored in a secured memory location, which

cannot be accessed by regular users. The capabilities stores are not pointed at user's segment table. At the time of execution, the capabilities of objects that need to be accessed are readily available. The restriction improvises the speed at which the objects can be accessed.

5. **Suggest an efficient scheme for maintaining a per-user protection scheme.That is, the system maintains one directory per user, and that directory lists allthe objects to which the user is allowed access. Your design should address the needs of a system with 1000 users, of whom no more than 20 are active at anytime. Each user has an average of 200 permitted objects; there are 50,000 totalobjects in the system.**

Per subject access control list is a best method in this scenario. This scheme allows access permission to 1000 users with 20 active at a single point of time. These users will have access to 50,000 objects. But the users can access 200 objects access only. This can be implemented with per subject directory list. In this way; a single user can get access to group protection scheme. The group will get right access to these objects.

6. Calculate the timing of password-guessing attacks:

(a) If passwords are three uppercase alphabetic characters long, how much time would it take to determine a particular password, assuming that testing an individual password requires 5 seconds? How much time if testing requires 0.001 seconds?

-The generated password has 3 characters for decoding. The total alphabets are 26,the possibility of password for 1 is 26^1, and same for 2 character length, it will be 26^2. In case of 3 characters password length it will be 26^3 password. The time taken for testing single password is 5 sec,

and then the time required for 26^3 password is 5*26^3 sec, which is equal to 87880 seconds, which is equal to 24.11 hours approximately.

(b) Argue for a particular amount of time as the starting point for "secure."

That is, suppose an attacker plans to use a brute-force attack to determine a password. For what value of *x* (the total amount of time to try as manypasswords as necessary) would the attacker find this attack prohibitivelylong?

- The password that consists of characters can be easily decoded. The secured password length should not be too short, and should be manipulated up to 8 characters. This 8 characters can brings the probability of 26^8, and decoding will take 66.22 years. This period is longer for secured point.

(c) If the cutoff between "insecure" and "secure" were *x* amount of time,how long would a secure password have to be? State and justify yourassumptions regarding the character set from which the password isselected and the amount of time required to test a single password.

-The secured password should be created with character length of 7 to 10 characters. The length of password determines the password security. The password is case sensitive, with special characters, and numerical can add more security to password.

7. Design a protocol by which two mutually suspicious parties can authenticateeach other. Your protocol should be usable the first time these parties try toauthenticate each other.

-The password can be applied to the files, and the access can be permitted only if the password is correct. The other method is cryptography in which the mutual parties can transmit, and access the data. The certificate based authentication will support the authentication between each other.

The Trusted Platform Module Technologies can be used for building the authentication between the two parties.

8. List three reasons people might be reluctant to use biometrics forauthentication. Can you think of ways to counter those objections?

-The people are reluctant to use biometric authentication, because the system captures the key biometric components, and the individuals are fear of misuse. The biometric machines some time show errors, even though the right person is accessing. This creates frustration, when the user wants to access. The biometric systems are not always accurate, and sometime two or three modes of biometrics are used for authentication. E.g. Iris andfinger prints are used in combination for authentication. This require body, or body part are contacted are exposed to radiation for reading. To counter these objections, the individuals are trained in using biometrics, and its correct method of usage for authentication. The use of biometrics is safe, and this should be communicated to the users, and encourage the biometrics implementation. The biometric data cannot be stolen, or forged and the authentication is always with the user.

9. False positive and false negative rates can be adjusted, and they are oftencomplementary: Lowering one raises the other. List two situations in which falsenegatives are significantly more serious than false positives.

- The false negative is more serious then false positives, for example if the credit card holders, card is not authenticated, or accepted because of false negative, then the user cannot buy the product or service. This raises the question on service provider credibility. The same example can be seen in another way, if the access is restricted in case of an emergency, then it will be serious loss.

10. In a typical office, biometric authentication might be used to control access toemployees and registered visitors only. We know the system will have some falsenegatives, some employees falsely denied access, so we need a human override,
someone who can examine the employee and allow access in spite of the failedauthentication. Thus, we need a human guard at the door to handle problems, as wellas the authentication device; without biometrics we would have had just the guard. Consequently, we have the same number of personnel with or without biometrics,plus we have the added cost to acquire and maintain the biometrics system. Explainthe security advantage in this situation that justifies the extra expense.

- The guard cannot be a replacement for the biometric system. The security guard helps the individuals, for which the access is a problem with biometrics. The security guard verifies the authenticity of access, and monitors the access at the door. This prevents the unauthorized access, and manages false negatives.