CS 562 Assignment 1 *Mithilaesh Jayakumar*
G01206238

1.2 Classify each of the following as a violation of confidentiality, integrity, availability, or of some combination (and state what that is).

(a) During the final examination, Alice copies an answer from another student's paper, then realizes that answer is wrong and corrects it before submitting her paper for grading.

This is a violation of Confidentiality because Alice copied data from another student.

(b) Bob registers the domain name AddisonWesley.com and refuses to let the publisher Addison Wesley buy or use that domain name.

This is a violation of Availability as the domain is not available to the publisher.

(c) Carol attempts to login to Dave's account, unsuccessfully guessing various passwords until the operating system locks the account to prevent further guessing (but also preventing Dave from logging in).

This is a violation of Availability as Dave does not have access to his account and also violation of Integrity as Carol is not supposed to alter Dave's account.

(d) Edward figures out a way to access any file on the University computer and runs a program that lowers the grades of some students he saw cheating earlier in the semester.

This is a violation of Confidentiality as Edward tries to access files in University computer and also violation of Integrity as Edward tries to change the data present in the University computer.

(e) Fran figures out a way to access any file on the University computer and runs a program that computes and reports to her the average homework grade of students in her security course.

This is a violation of Confidentiality as Fran tries to access files in the University computer.

(f) George uses an extension to listen-in on his brother's telephone conversation and accidentally forgets to hang-up the phone when he is done listening.

This is a violation of Confidentiality as George listens to his brother's telephone conversation and also violation of availability as he forgets to hang up the phone making it unavailable for others to use.

1.3 What kind of security property is each of the following?

(a) The grade for the assignment is available only to the student who submitted that assignment.

Confidentiality

(b) If your course grade changed, then the professor made that change.

Integrity

(c) The output is produced by the CS Department web server.

Availability

(d) Requests to the web server are not processed out of order.

Availability

(e) No run-time exception is raised during execution.

Availability

(f) User Alice may not issue read operations to file F .

Confidentiality

(g) The program Alice runs to issue read operations on file F runs to completion.

Availability

(h) If Alice sends a piece of email then there is no way for her to deny having done so.

Integrity

(i) The downloaded piece of music may be played at most 5 times.

Availability to the person who tries to downloaded the music. Confidentiality to the owner/ source of the music with a play limit of 5 times.

(j) The memo may be forwarded to your employees but they may not forward it any further

Confidentiality

1.8 Consider an enlightened company, where employees who have free time may use their office computers to access the Internet for personal tasks. A newspaper article causes management to fear that the company's secret documents are being leaked to the press, and that prompts an audit to identify which employees have electronic copies of secret documents. To implement that audit, the security officer proposes that a virus be written and used to infect all machines on the company's intranet. That virus would behave as follows.

1. This virus periodically scans the disk of any machine it infects, locating any secret documents being stored there.
2. Whenever the virus locates a secret document, it sends email containing the name of the machine and secret document to the security officer.

Discuss whether this scheme violates employee privacy.

This scheme does not violate any employee privacy as the computers used by them are owned by the company. The company has the right to deploy virus into their employee's computer to identify the cause for the issue.

This would become a privacy issue only if the virus is deployed into the employee's personal computers as this would lead to violation of confidentiality by accessing their personal files.

7.7 Consider a collection of fine-grained objects Obj 1 , Obj 2 , ..., Obj n . A set Privs i of privileges is associated with accesses to object Obj i , and an access control policy is specified in terms of an authorization relation Auth and set C of commands. Given is a system that (only) supports access control for relatively coarse-grained objects, Obj 0 1 , Obj 0 2 , ... Obj 0 m where m < n holds. Suppose each coarse-grained object groups a set of fine-grained objects. Describe an authorization relation Auth 0 , set C 0 of commands, and sets Privs 0 i of privileges for each Obj 0 i to ensure that the authorization requirements imposed by the original fine-grained access control restrictions will still be enforced.

We can use protection domains to apply more fine grained controls on coarse grained objects. We can define privileges on those protection domains based on the least privilege principle. All of the individual fine grained objects (obj) should have access to privileges (priv') when they are in coarse grained objects (obj'). By this way all fine-grained objects (Obj) in a coarse group object (Obj') still have the same privileges (Priv or Priv') while allowing for Coarse grained authorization on a set C and reducing the length of our access control list .

7.10 An access control list

<P 1 , Privs 1 > <P 2 , Privs 2 > . . . <P L , Privs L >

is defined to have length L provided i =/= j implies P i =/= P j . Consider the possible access control lists for an object that appears in a system with n principals, where there are m different kinds of privileges.

(a) If the system does not include support for groups, then what is the longest possible access control list?

The longest access control list will be n*m long

(b) Suppose n > m holds and the system includes support for groups comprising subsets of the original n principals. Then (i) what is the longest access control list possible and (ii) is it ever necessary to construct that list if our concern is with access authorization but not with review of privileges or with changes to group compositions or to the privileges granted to each principal?

The longest access control list will be (g + n)*m where g is the number of groups. If our concern is only access and not privilege then its not necessary to construct such a long list

(c) Suppose n < m holds and the system includes support for groups comprising subsets of the original n principals. Then (i) what is the longest access control list possible and (ii) is it ever necessary to construct that list if our only concern is with access authorization but not with review of privileges or with changes to group compositions or to the privileges granted to each principal?

The longest access control list will be n+g where g is the number of groups. If our concern is only access and not privilege then its not necessary to construct such a long list

7.12 Instead of storing ACL-entries hP i , Privs i i in a list, we might employ a data structure that supports having principal names be retrieval keys. What are the advantages and disadvantages of the following candidates.

(a) Hash table.

Advantages:

- ***Hash table is faster, cheap and easy to implement***

Disadvantages:

- ***It requires lot of memory to cover the range of hashes and a good hash function.***
- ***Rehashing is also very expensive***

(b) Binary search tree.

Advantage:

- ***It performs searching very fast with faster insertion of data and allows creation of memory as we need.***

Disadvantages:

- ***Implementation is complex and takes more time for deletion of data.***