Name: Subhendu Maji
Roll: 18ETCS002121

Subject code: 19CSC315A
subject name: Information Security and Protection

Date: 21-05-2021

CSE-C Section

TT1

2.

3. a) The basic components of security & protection of information ⇒ information system are –

(i) Confidentiality

confidentiality is concealment of information or resources.

Confidential information includes.

- sensitive information.
- personal records
- proprietary information
- trade secrets etc.

The origin is Need-to-know principle.

confidentiality is supported by Access control mechanism.

(ii) Integrity

Integrity refers to trustworthiness of data or resources. In terms of preventing improper or unauthorized modification or change.

This includes –

- data integrity: content of information.
- origin integrity: source of information. (authentication).
-

eg. A news item prints as received a leaked information but attributes it to a wrong source.

Integrity mechanism includes -

- Prevention mechanisms
  - prevent unauthorised users from accessing information (also ~~modify~~ modifying data in unauthorized manner).

- Detection mechanisms.
  - only report if data is not trustworthy.
  - Either report cause of integrity violation or only report a violation.
- Do not prevent violations of integrity.

Integrity is affected by origin of data, how well data is protected along the path.

(iii) Availability

Availability is the ability to use information or resources.

- Relavence to security.
  - Deliberate denial of access of data or service making it ~~unavailbo~~ unavailable or unusable

- Compromising availibility : denial of service (DOS)
  - Manipulate use/control parameters so that the statistical model is invalid.
  - Availability mechanisms fail as the environment is now changed.

Detection of DOS is difficult as it may look like an ~~ordy~~ atypical event.

Name : Subhendu Maji Roll : 18ETCS002121 (3)

2.

b)

a) Lina copies Anil's assignment

confidentiality, ~~[illegible]~~

b) Deepak crashes Vibha's computer.

availibility, integrity

c) Frank alters the online invoice of Leena from Rs 100 to Rs. 1000.

Integrity, ~~[illegible]~~

d) Sharat acquires Deepa's IP address to access her computer..

Integrity,
confidentiality, ~~[illegible]~~.

Name : Subhendu Maji Roll : 18ETCS002121

3.

a)

A security policy is a statement of what is, and what is not, allowed.
Breaking a security policy leads to security breach.

a security mechanism is a method, tool, or procedure for enforcing a security policy.

Eg.

a security policy prohibits any student from copying another student's homework.

a security mechanism like computer mechanism prevent others from reading a user's file.

Eg: If ~~person~~ student A did not protect his ~~files~~ files. and student B copies his homework. Student B has violated the security policy. Student A's failure does not give authorize Student B to copy the files.

3.

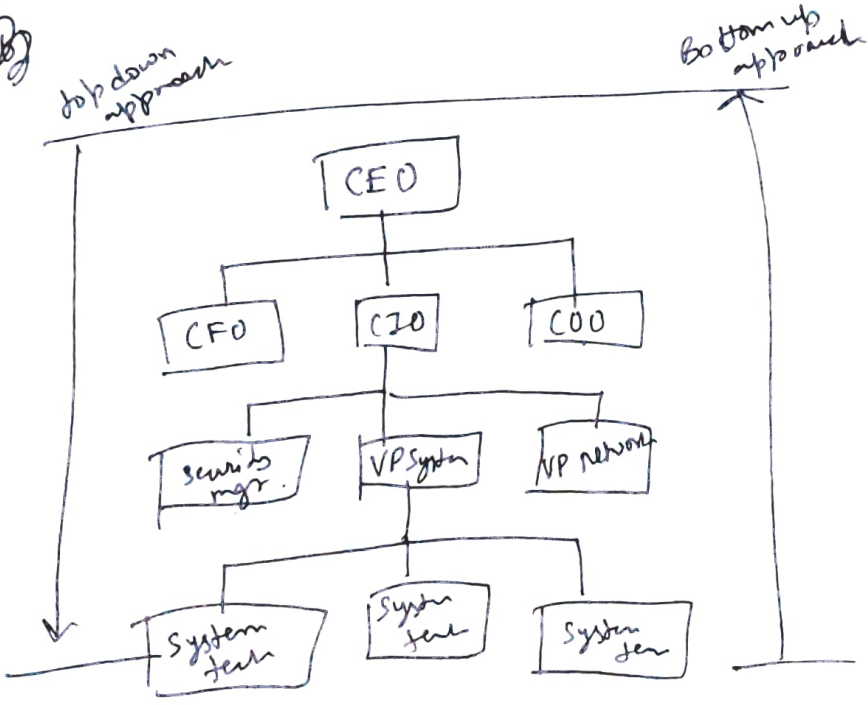
b) Top down vs. bottom up.

(i) The top down approach analyzes risk by aggregating the impact of internal operational failures while the bottom up approach analyzes the risks in an individual process using models.

(ii) The top down approach doesn't differentiate between high-frequency low severity vs low-frequency high severity events while the bottom-up approach does.

(iii) The top down approach is simple & not data-intensive whereas the bottom up approach is complex as well as very data-intensive.

(iv) Top down approaches are backward looking while bottom up approaches are forward-looking.



Name: Subhendu Maji

ROLL: 18ETCS002121

4).

a) Access control Matrix

(i)

	traffic.doc	status.doc	action.doc
Adarsh	owns, read, write		read
Bala	read	owns, read, write	
Chandan			owns, read, write

(ii) Chandan gives

Bala permission to read action.doc

Adarsh removes Bala to read traffic.doc

New access control matrix

	traffic.doc	status.doc	action.doc
Adarsh	owns, read, write		read
Bala		owns, read, write	read
Chandan			owns, read, write

4. b)

```
command  copy-rights(P,Q,O)
    create object O;
    enter own into A[P,O];
   if [read, copy] in A[P,O]
        then
            enter read in A[Q,O];
   if [write, copy] in A[P,O]
        then enter write in A[Q,O];
   if [execute, copy] in A[P,O]
      then
          enter exeute in A[Q,O];

  end.
```

Name : Subhendu Maji Roll : 18ETCS002121 (8)

5 a)

given,

users = A, B, C

resources = X, Y, Z

Access Control Matrix

	X	Y	Z
A	read, write, execute	read	
B		read, write	~~read~~ read, execute
C		read, write	read

b) given,

users	group
A	athelete, musician
B	musician
C	athelete

Updated Access control Matrix.

	X	Y	Z
A	read, write, execute	read, execute	
B		read, write, execute	read, execute
C	write	read, write	read

i) Subject C is allowed to write to object X : True

ii) Subject A is allowed to execute object Y : True

Name : Subhendu Maji. Roll : 18ETCS002121 (10)

1.

A threat is a potential violation of security.

Common security threats are —

(i) Snooping or Eavesdropping

Snooping is unauthorized interception of information. It is a form of disclosure.

Some passive entity of snooping are—

- Listening to communication.
- Browsing through files.
- Reading system information.

Passive wiretapping is snooping where a network is monitored.

Some examples are —.

(i) passwords stored unencrypted in plain text-

(ii) passwords exchanged on a wireless channel with weak / broken encryption.

(iii) over the shoulder browsing.

(ii) Modification or alteration.

Modification is change of information.

It covers three classes of threats

- Deception : modified data is used to determine action to be taken
- Disruption & Usurption : Modified data is used to control system operation.

active : results from an entity changing information.

Active wiretapping is ~~data~~ ~~control~~ alteration of data moving across a network.

eg: Man in the Middle (MOM) attack

An intruder reads messages from the sender & sends (possibly modified) versions to the recipent, in hopes that the recipent & sender will not realize the presence of the intermediary.

Integrity servics counter this threat.

(iii) Masquerading or Spoofing

Masquerading is impersonation of one entity by another. It is a form of both deception and usurption.

It is luring a victim into believing that the entity with which it is communicating is a different entity.

Eg: (i) A user tries to log into a computer across the internet but instead reaches another computer that claims to be the desired one.

(ii) A user tries to read a web page, but an attacker has arranged for the user to be given a different page.

A passive attack is the user simply accesses the web page.

often an active attack, the attacker responses dynamically to mislead the user about the web page

Often is an usurpation, used to usurp control of a system by an attacker impersonationating an authorized manager or controller.

Integrity services counter this threat is called authentication services.