1. Give an example of a situation in which a compromise of confidentiality leads to a compromise in integrity; and then give an example of a situation in which a compromise of integrity leads to a compromise in confidentiality.

Answer:

There are multiple cases where in confidentiality can lead to a compromise in integrity.

Let us consider, Person A has acquired password of a bank account of Person B. As password is considered to be sensitive information pertaining to Person B, there is a **compromise of confidentiality** when Person B is acquiring it. There could be multiple ways using which he could acquire this, either by hacking or trying to break the password generator algorithm for the system. Person A logs in to the bank account using same password and changes the information of Person B. Person A can change address or date of birth or any other sensitive information present on the system. Therefore, resulting in **compromising the integrity.**

Example where in integrity leads to compromise in confidentiality.

Let us consider a client-server system where client will be sending some information such as function or REST API information using which the server will make certain calculations. But, there happens a situation where the passing information gets compromised and has been modified in transmission. Some how the transmission channel loses its protection/firewall thereby leading to invite attackers to change passing information easily. At the same time, the server is not aware of such attack/issue and assumes the function / REST API information is sent by authenticated client only. There isn't any way for the server as well to verify the same. The system uses same function/REST API information and calculates the results which are to be given to clients are sensitive for the company. Along with, the attacker has made the function/REST API in such a way- that it also sends the results to him via mail or any other way.
Therefore, here we can say that – the compromise happened by changing the information during transmission leads to **compromise in integrity** and as the system uses same formulae to calculate sensitive results which are again sent to attacker without prior knowledge of server system leads to **compromise in confidentiality**.

2. Classify each of the following as an example of a mandatory, discretionary, or originator controlled policy, or a combination thereof. Justify your answers.

a. The file access control mechanisms of the LINUX operating system.
Answer:
Discretionary, mandatory and originator-controlled policies i.e. combination of all three applies to LINUX.

Justification:

Discretionary – User in Linux can set permissions of change the permissions of a file using chmod command.

Mandatory – There are certain files in Linux which cannot be altered by user. For example, a kernel file itself or other boot files which does not allow to be edited by a user.
Originator – A user who creates the file can always decide the access permissions he can give for the file. Because, his ID was allowed to create the file, therefore he can change and provide access permissions as well.

b. A system in which no memorandum can be distributed without the author's consent.
Answer:

Justification:
Originator – It takes into account only the permissions provided by the author, Therefore it follows originator controlled policy.

c.A military facility in which only generals can enter a particular room.

Answer:
Justification:

Mandatory - The military system itself has designed the access control mechanism and it cannot be altered by any individual. Only the people who has been given access by the system are allowed to enter the room. Therefore, the system has the power to decide on the access policies. Therefore, such type of policy is mandatory access control policy.

d. A university registrar's office, in which a faculty member can see the grades of a particular student provided that the student has given written permission for the faculty member to see them.
Answer:
Discretionary - "Provided" keyword plays an important role here. It tells that, the faculty member can see the grades of a particular student only if and if – the student has given written permission. That means, the student has the sole authority to give a permission or not to give. Without permission, the facult y member has no right/access to do so. Therefore, as student has complete control over the access mechanism – such type of policy is said to be discretionary access control policy.

3. Given the security levels TOP SECRET, SECRET, CONFIDENTIAL, and UNCLASSIFIED (ordered from highest to lowest), and the categories A, B, and C, specify what types of access (read, write, both, or neither) is allowed in each of the following situations. Justify your answers by applying the definition of the dominate relationship. Assume that discretionary access controls allow anyone access unless otherwise specified.

a. Paul, cleared for (TOP SECRET, {A, C}), wants to access a document classified (SECRET, {B, C}).

Here,
Paul's clearance which is TOP SECRECT > object's classification SECRET.
But, object's category i.e. {B, C} is not subset of Pauls' category i.e. {A, C}. Hence, **Paul would not be able to read the object document as Paul does not dominate object document.**
Document classification is SECRET < clearance of Paul i.e. TOP SECRET, therefore, document does not dominate subject as well. **Hence, Paul would not be able to write the object document.**

b. Anna, cleared for (CONFIDENTIAL, {C}), wants to access a document classified
(CONFIDENTIAL, {B}).

Here,
Anna's clearance which is CONFIDENTIAL = objects classification CONFIDENTIAL.
But, object's category i.e. {B} is not subset of Anna' s category i.e. {C}. Hence, **Anna would not be able to read the object document as Anna does not dominate object document.**
Document classification is CONFIDENTIAL = objects classification CONFIDENTIAL.
But, Document's category i.e. {B} should be subset of subject's category i.e {A} which is not. Hence, **subject would not be able to write the object document.**

c. Jesse, cleared for (SECRET, {C}), wants to access a document classified (CONFIDENTIAL, {C}).

Here,
Jesse clearance which is SECRET > objects classification CONFIDENTIAL.
Also, of object's category i.e. {C} is subset of Jesse s category i.e. {C}. Hence, Jesse **would be able to read the object document as Jesse does dominate object document.**
Document classification is CONFIDENTIAL < Jesse's clearance.
Therefore**, Jesse would not be able to write the document as there is document does not dominate subject i.e. Jesse**.

d. Sammi, cleared for (TOP SECRET, {A, C}), wants to access a document classified
(CONFIDENTIAL, {A}).

Here,
Sammi clearance which is TOP SECRET > objects classification CONFIDENTIAL
Also, object's category i.e. {A} is subset of Sammi s category i.e. {A, C} should be which is present. Hence, **Sammi would be able to read the object document as Sammi does dominate object document**.

Document classification is CONFIDENTIAL < Sammi's clearance i.e. TOP SECRET.
Therefore, Sammi would not be able to write the object document as document does not dominate the subject.

e. Robin, who has no clearances (and so works at the UNCLASSIFIED level), wants to access a
document classified (CONFIDENTIAL, {B}).

Here,
Robin clearance which is UNCLASSIFIED < objects classification CONFIDENTIAL.
Hence, **Robin would not be able to read the object document as Robin does not dominate object document.**
Document classification is CONFIDENTIAL > robin's clearance i.e. UNCLASSIFIED. Therefore, **robin would be able to write the document because document dominate Robin.**

4. Suppose a system implementing Bell-LaPadula's model used the same labels for security levels and categories as for integrity levels and categories under the Biba model, which the system implemented. Under what conditions could one subject read an object? Write to an object?

Bell-LaPadula Model is based on "no read up and no write down" whereas the Biba integrity model is based on "no read down and no writes up".

For example, consider subject S with labels (L,K) and object O with labels (L',K').
Below four cases would appear

1. As per Bell-LaPadula model,
   If S dominates O, then S can read the object O but,
   S cannot write the object O.
   Opposite to that, in case of Biba integrity model,

   **If S dominates O, then S cannot read the object O but,
   S can write the object O.**

2. As per Bell-LaPadula model,
   If O dominates S, then S can write on object O but,
   S cannot read on object O.
   Opposite to that, in case of Biba integrity model,

   **If S dominates O, then S cannot write on object O but,
   S can read the object O**.

3. Similarly,
   **If both subject and object i.e S and O are at same security levels, i.e S=O,
   L = L' and K' = K , then according to model - S can do both read and write to object O.**

4. Also,
   No dominating relation between S and O – then according to model – S cannot do both read and write to object O.

5. A physician who is addicted to a pain-killing medicine can prescribe the medication for herself. Please show how RBAC in general, and Definition 7-11 on page 94 of the textbook specifically, can be used to govern the dispensing of prescription drugs to prevent a physician from prescribing medicine for herself.

Based on the trainer example provided in the textbox, there exists some roles which subsume others. Here also, the same scenario persists where the physician is treating him/her self-assuming two kind of roles 1. physician 2. Patient.

This is nothing but containment where hierarchy of roles exists moving around physician and patient.

Similarly, based on the next example provided in the textbox, RBAC can model the separation of duty rule. The key is to recognize that the users in some roles cannot enter other roles.
i.e. according to definition 7-11
Let r be a role and let s be a subject such that if r belongs to authorized set of roles that s scan take, then the predicate meauth(r) (for mutually exclusive authorizations) is the set of roles that s cannot assume.

Here, by applying above **rule of separation of duty**, we can say that the physician cannot assume the role of her own patient. Therefore, she cannot prescribe medicine for herself. The principle of “Separation of duty” prevents a physician from prescribing medicine to herself.