ITIS6200 EXERCISE: 02

Amaan syed (asyed15@uncc.edu)

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

- **The file access control mechanisms of the LINUX operating system.**

This is categorized as a discretionary controlled policy because the user who creates the file must decide on the access that can be provided to other users.

- **A system in which no memorandum can be distributed without the author's consent.**

This is categorized as an Originator-controlled policy, author (the originator) has control over the distribution of their work (the memorandum). This is so that, should we draft a memorandum, we may state that just our information would be shared with others.

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

This is categorized as a Mandatory Controlled policy. The access that the system commands cannot be altered by an individual. In certain complicated situations, the decision to promote personnel to the rank of "general" may be made at the discretion of the military facility's owner. In that case, the owner would be able to authorize access to the military facility.

2. The Bell-LaPadula model is used to enforce information confidentiality through controlling the data flow direction. In short, it can be summarized as "no read up, no write down". To define the "up" and "down" in the system, the model introduces the relationship of "Domination" in security levels. The security level (L1, C1) dominates the security level (L2, C2) if and only if $L2 \leq L1$ and $C2 \subseteq C1$. Here L1 and L2 represent security clearance levels, and C1 and C2 represent subsets of categories to which the data belongs. 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.

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

  Paul cannot access the document. Paul cannot read and write the document. Here, L1 = Top Secret C1 = {A, C} L2 = Secret C2 = {B, C} ⇒ L2 < L1; C2 ⊄ C1. Therefore, (L1, C1) does not dominate (L2, C2).

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

  Here, L1 = Confidential C1 = {C} L2 = Confidential C2 = {B} ⇒ L2 = L1; C2 ⊄ C1. Therefore, (L1, C1) does not dominate (L2, C2). So, Anna cannot access the document. Anna cannot read and write the document.

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

  Jesse can access the document. Here, L1 = Secret C1 = {C} L2 = Confidential C2 = {C} ⇒ L2 < L1; C2 = C1 Therefore, (L1, C1) dominates (L2, C2). According to the Bell-LaPadula model, there is “no read up, no write down”. Since the level of the document is lower than the person, Jesse can read the document but cannot write to it.

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

  Here, L1 = Top Secret C1 = {A, C} L2 = Confidential C2 = {A} ⇒ L2 < L1; C2 ⊂ C1 Therefore, (L1, C1) dominates (L2, C2). That is why, Sammi can access the document. Sammy’s clearance level dominates the document but cannot write the document because of no write-down and Sammi’s clearance level TOP SECRET > documents CONFIDENTIAL.

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

  Here, L1 = Unclassified C1 = {} L2 = Confidential C2 = {B} ⇒ L2 > L1; C2 ⊄ C1 Therefore, (L1, C1) does not dominate (L2, C2). Hence, (L1, C1) does not dominate (L2, C2). The document cannot be read by Robin since "no read up, no write down", and Robin's level is lower than the documents. But since the document’s level dominates Robin, she is allowed to write the document.

3. The Bell-LaPadula model is used to enforce information confidentiality through controlling the data flow direction. In short, it can be summarized as “no read up, no write down”. To define the “up” and “down” in the system, the model introduces the relationship of “Domination” in security levels. The security level (L1, C1) dominates the security level (L2, C2) if and only if L2 ≤ L1 and C2 ⊆ C1. Here L1 and L2 represent security clearance levels, and C1

and C2 represent subsets of categories to which the data belongs. Assume that we have a system with four levels of security clearance: Top Secret (TS), Secret (S), Classified (C), and Unclassified (U), from high to low. The system also has three categories: Army, Navy, and Air Force. Please fill "dominate" or "not dominate" in the following blanks. (It reads as "the left side dominates (or not dominates) the right side".)

- **Classified, {Army, Navy}) Dominate (Unclassified, {})**
- **(Top Secret, {Army, Air}) Not Dominate (Secret, {Army, Navy})**
- **(Secret, {Army, Navy, Air}) Dominate (Secret, {Air, Navy})**
- **(Secret, {Navy, Army}) Not Dominate (Top Secret, {Army, Navy})**

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?

In a system where both the Bell-LaPadula (BLP) model and the Biba model are executed with the same labels for security levels and categories, certain conditions must be met for a subject to read or write to an object.

Read Access (BLP Model):

According to the Bell-LaPadula model, a subject can read an object if the subject's security level overwhelms the object's security level. In other words, the subject's security clearance must be equal to or higher than the security classification of the protest. This is often known as the Simple Security Property (SSP).

Write Access (Biba Model):

Within the Biba model, subjects can write to an object if the object's integrity level dominates the subject's integrity level. This guarantees that data streams in a way that keeps up integrity.

Now to analyze under what conditions one subject might read an object and write to an object:

Read Access:

On the off chance that the security level of the subject breaks even with to or higher than the security level of the object, as per the BLP model, the subject could read the object.

Write Access:

If the integrity level of the object breaks even with or higher than the integrity level of the subject, as per the Biba model, the subject could write to the object.

Given that both the security and integrity labels are the same, for a subject to read an object, the subject's label must dominate the object's label. Additionally, for a subject to write to an object, the object's label must dominate the subject's label.

Therefore, the conditions for a subject to read or write to an object are:

Read Access: Subject's label ≥ Object's label

Write Access: Object's label ≥ Subject's label

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.

RBAC's ability to enforce the separation of duties concept enables it to regulate the distribution of prescription drugs, preventing doctors from self-prescribing. This is accomplished through RBAC's central definition of duty separation, which restricts individuals in one role from performing tasks associated with another. By assigning responsibilities to two distinct roles, r1, and r2, RBAC ensures that no single person can take on both roles simultaneously. This is expressed as let meauth(r1) = {r2}, ensuring that authr(s) doesn't include both r1 and r2 at the same time. $(\forall s \in S)$ [r1 $\in$ authr(s) $\rightarrow$ r2 $\notin$ authr(s)]. Let r represent a role and s a subject, with r being an authentic role for s. When authorizations are mutually exclusive, the set of roles that s cannot take on due to the separation of duties requirement is defined by the predicate meauth(r). $(\forall$ r1, r2 $\in$ R) [r2 $\in$ meauth(r1)

$\rightarrow (\forall s \in S)$ [r1 $\in$ authr(s) $\rightarrow$ r2 $\notin$ authr(s)]].