Exercise-2

Vineeth Mylavarapu
ID.801337050
College of Computing and Informatics

1. Question-1

A. The file access control mechanisms of the LINUX operating system

Restricting Access to objects specific to individual or groups are configured by Root user while giving access. Here in LINUX user is going to create file and access control as per his required users, since this condition will be **Discretionary Access Control.**

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

Any File of Application has its own privileges where owner will have access to modify data internally. No other than Authorized Personnel will have access to that specific data other than creator. Also, it cannot be broadcasted without his notice. Hence this will be considered as **Originator controlled access control.**

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

This is clear case of **Mandatory Access control** where this is classified into one of the restricted/secret and it is centralized security. In our case generals are marked as secret/high authority to allow individuals into that room.

2. Question-2

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

L1 -> Top Secret, C1 -> {A, C}
L2 -> Secret, C2 -> {B, C}

$\Rightarrow L2 < L1; C2 \not\subset C1$

Hence, (L1, C1) have not dominated (L2, C2). So, Paul cannot open the document as well as cannot read and write to the document.

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

L1 -> Confidential, C1 -> {C}
L2 -> Confidential, C2 -> {B}

$\Rightarrow L2 = L1; C2 \not\subset C1$

Here, (L1, C1) do not dominate (L2, C2). So, Anna cannot access the document as well as cannot read and write to the document.

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

L1 -> Secret, C1 -> {C}
L2 -> Confidential, C2 -> {C}

$\Rightarrow L2<L1; C2= C1$

Here, (L1, C1) dominating (L2, C2). So, Jesse can access the document. As per, Bell-LaPadula model there is "no read up, no write down". So the level of the document is lower than the person, Jesse can read the document but cannot write to it.

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

L1 -> Top Secret, C1 -> {A, C}

L2 -> Confidential, C2 -> {A}
$\Rightarrow L2 < L1; C2 \subset C1$

Hence, (L1, C1) dominates (L2, C2). Therefore, Sammi will access the document. Because of "no read up, no write down", and permission of the document is lower than Sammi, he can read the document but cannot write to it.

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

L1 -> Unclassified, C1 = {}
L2 -> Confidential, C2 = {B}

$\Rightarrow L2 > L1; C2 \not\subset C1$

Therefore, (L1, C1) is not dominating (L2, C2). Because of "no read up, no write down", and permission level of the document is lower than Robin, she cannot read the document. But since the document's level dominates Robin, she is allowed to write to the document.

3. Question-3

a. (Classified, {Army, Navy}) **dominating** (Unclassified, {})

b. (Top Secret, {Army, Air}) **not dominating** (Secret, {Army, Navy})

c. (Secret, {Army, Navy, Air}) **dominating** (Secret, {Air, Navy})

d. (Secret, {Navy, Army}) **not dominating** (Top Secret, {Army, Navy})

4. Question-4

A. In this scenario only one subject needs to read an object:

- As per Biba model the object integrity should be dominated the integrity level of the subject.
- Subject Integrity Level ≤ Object Integrity Level: no read down
- In the Bell-LaPadula model the clearance level of the subject needs to dominate the categorized object level.
- Security clearance level of Subject ≥ Classification level of Object: No read up
- Here security levels and categories are same as clearance levels and categories, it is possible for a subject to read an object only if the subject and object are of same level.
- Level of Subject = Level of Object.

B. For a scenario where one subject needs to write an object:

- According to Biba model the subject integrity should dominate the integrity level of the object.
- Subject Integrity ≥ Object Integrity: no write up
- In the Bell-LaPadula model the clearance level of the object must dominate the classification level of the subject.
- Security clearance level of Subject ≤ Classification level of Object: no write down
- Hence the security levels and categories are same as clearance levels and categories, it is possible for a subject to read only if the subject and object are of same level.
- Subject Level = Object Level.

5. Question-5

RBAC- Role Based Access Control

The Use case of implementing and configuring multiple policies and procedures as per the user’s requirements up to their appropriate usage. RBAC deals with access privileges of the individual users and their requirements.

RBAC is mainly used in the large organizations where multiple teams have their own resources and access to them. Also, RBAC should restrict access to resources of the other teams who are not responsible for accessing those data.

Here, physician role and the duties she can perform can be modified as per the situation, so that the activity “prescribing medicine for self” is in a mutually exclusive rules that the physician is not authorized to do. Hence, she cannot prescribe the medicine to herself.

Assume,

r1= consumer of painkilling medicine

r2= painkilling medicine prescription

meauth (r1) = [r2], here authr (s) shouldn’t contain both r1, r2

$$(\forall r_1, r_2 \in R)\ [r_2 \in meauth(r_1) \rightarrow [(\forall s \in S)\ [r_1 \in authr(s) \rightarrow r_2 \notin authr(s)]]]$$