

# Task1

## Q1

### Solution:

Given the security levels and category set in terms of confidentiality and integrity. (there are three security levels L1, L2, L3 such that L3 is the highest and L1 is the lowest permission classification)

Type	Name	Confidentiality Level
subject	$S_1$	$L_1(A, B)$
subject	$S_2$	$L_2(A, C)$
subject	$S_3$	$L_3(B)$
subject	$S_4$	$L_2(C, B)$
subject	$S_5$	$L_2(B)$
object	$O_1$	$L_2(A, B, C)$
object	$O_2$	$L_1(A)$
object	$O_3$	$L_3(A, C)$
object	$O_4$	$L_2(\emptyset)$

Table 1: Confidentiality Properties

Type	Name	Integrity Level
subject	$S_1$	$L_1(X)$
subject	$S_2$	$L_2(Z)$
subject	$S_3$	$L_3(Y)$
subject	$S_4$	$L_2(X, Y)$
subject	$S_5$	$L_2(Z)$
object	$O_1$	$L_2(X, Y, Z)$
object	$O_2$	$L_1(X)$
object	$O_3$	$L_3(X)$
object	$O_4$	$L_2(\emptyset)$

Table 2: Integrity Properties

We use access rights calculated from BLP and Biba models then cross reference with given ACM to derive final output.

Properties covered:

- BLP
  - **simple security** - no read up
    - iff  $L(o) \leq L(s)$ , and  $C(o) \subseteq C(s)$
  - **star** - no write down
    - iff  $L(s) \leq L(o)$ , and  $C(s) \subseteq C(o)$
- Biba
  - **simple integrity** - no read down
    - iff  $i(s) \leq i(o)$ , and  $C(s) \subseteq C(o)$
  - **integrity star** - no write up

- iff  $i(o) \leq i(s)$ , and  $C(o) \subseteq C(s)$

Output of MAC:

\	O1	O2	O3	O4
S1	rw	rw	r	-
S2	rw	r	w	rw
S3	-	-	-	rw
S4	rw	w	-	rw
S5	rw	-	-	rw

Final output while taking DAC into consideration:

\	O1	O2	O3	O4
S1	rw	r	-	-
S2	-	r	w	r
S3	-	-	-	w
S4	rw	-	-	r
S5	rw	-	-	rw

## Task2

From the task context, it is known that given integrity star property i.e. no write up allowed (iff  $i(o) \leq i(s)$ , and  $C(o) \subseteq C(s)$ )

Access right for a user  $s_\alpha$  could be expressed as  $L2\{A, B\}$ . And has write access to object  $o_\beta$  -  $L1\{A\}$ .

### Q1

If the category set of  $o_\beta$  is changed to  $\emptyset$ , what is the consequence of this action?

**Solution:**

If the category set is changed to empty set, the access right (write) of user  $s_\alpha$  to the object would not be changed, as the user still dominates the object, and integrity level  $i(o) \leq i(s)$  remains.

## Q2

In addition to the changes in Q1, if the simple security property is applied to the scenario, what is the consequence of this action?

### Solution:

After the category set is changed to empty set, if the simple security property is applied and using the same category set for confidentiality.

As the confidentiality property of the user could be expressed as  $L2\{A,B\}$  and that of the subject as  $L1\{\emptyset\}$ . Consider the simple security property, the subject dominates the objects and  $L(o) \leq L(s)$  holds. So a read access of user  $s_\alpha$  to object  $o_\beta$  is granted.

## Q3

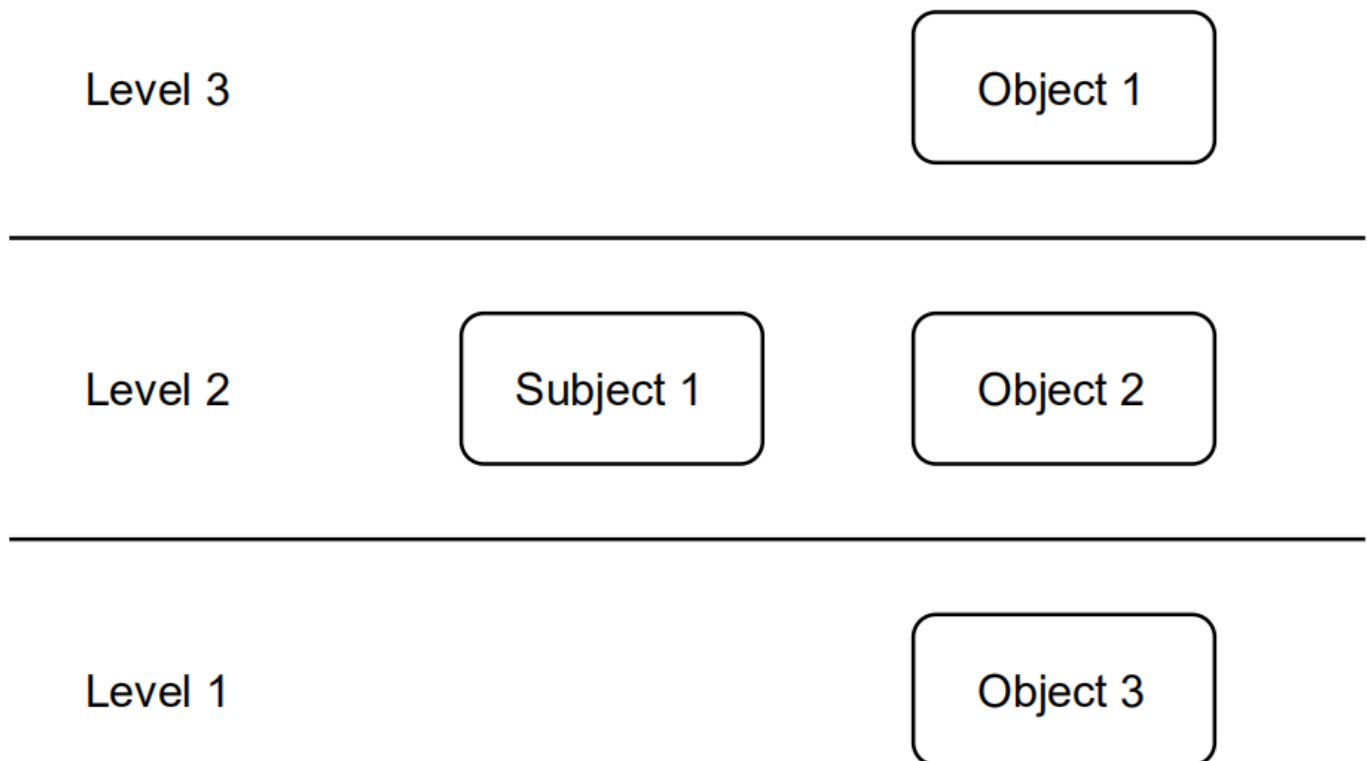


Figure 1: Security Model Example 1

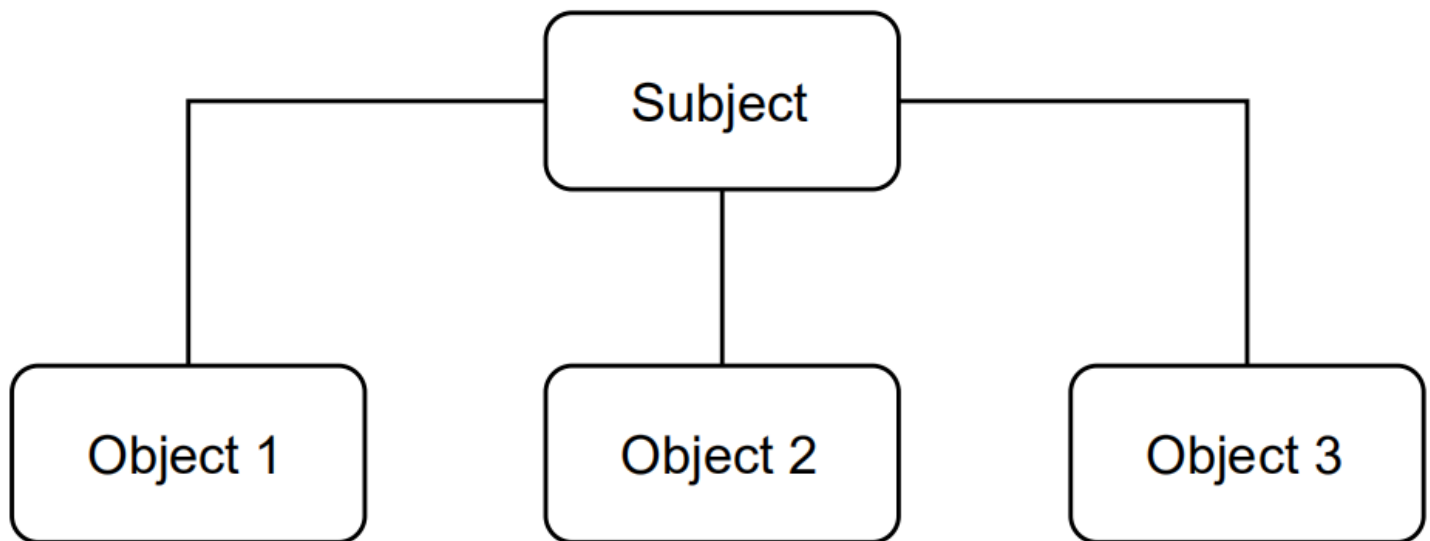
### Solution:

It is known that Low Watermark Policy for Objects has no restrictions on subjects to modify any objects, any subjects can modify any objects regardless of integrity level. So

S1 has write accesses to O1, O2, O3

And Low Watermark Policy for Objects has no effect on Invocation Property ( $s_1 \in S$  can invoke  $s_2 \in S$  iff  $i(s_2) \leq i(s_1)$ ). So if this model involves other subjects with integrity level less or equal than L2, then subject 1 can invoke them. Though there are no other subjects in this model.

#### Q4



## Figure 2: Security Model Example 2

What two BLP/Biba properties have been applied to this model in the event the following relations are observable with respect to the aforementioned constraints?

- Subject r Object 1
- Subject w/r Object 2
- Subject w/r Object 3

#### Solution:

Given the question context, it is known that the security levels of Subject and Object 1 is not the same, i.e.  $L(s) \neq L(o_1)$  while Subject has the same security levels with Object 2,3 i.e.  $L(s) = L(o_2) = L(o_3)$ . Also, security level of Object 1 dominates Object 2 i.e.  $L(o_2) < L(o_1)$  holds

From the constraints, **simple integrity property** could be applied here. Since no read down is allowed and subject has the same security levels with object 2,3 so  $i(s) \leq i(o_2)$  and  $i(s) \leq i(o_3)$  holds. Additionally, security level of Object 1 dominates Object 2 i.e.  $L(o_2) < L(o_1)$ , so  $i(s) < i(o_1)$  holds. Subject has read rights to all the objects.

Also, we apply the **integrity star property** on the model, so if subject has been granted write rights to Object 2, 3 it means that  $i(o_2) \leq i(s)$  and  $i(o_3) \leq i(s)$  holds. Since the security level of Object 1 dominates that of Object 2 i.e.  $i(o_2) < i(o_1)$ , and subject has the same security levels with Object 2,3, then  $i(s) < i(o_1)$ , which the relation "Subject r Object 1" holds (as subject has no write right to object 1).

As we know that by the simple security property of BLP model, where no read up is allowed, and security level of Object 1 dominates Object 2 i.e.  $L(o_2) < L(o_1)$ , however, subject should have read right to object 1 which requires  $L(o_1) \leq L(s)$ , so there exists the contradiction as the security levels of subject and  $o_1$  is not the same and  $o_1$  has higher level. Obviously, we cannot apply BLP model properties on this model.