Access Control Exercises

Q1. Compute the access matrix that results from the following initial state

	File 1	File 2	Process 1
Alice			
Bob		own	own
Charlie	own	*read	
David			

by executing the sequence of commands α defined as follows:

1 $CONFER_{*read}(Charlie, Alice, File1)$

2 $CONFER_{exec}(Bob, Alice, Process1)$

3 $CONFER_{write}(Charlie, Alice, File1)$

4 $CONFER_{read}(Bob, Bob, File2)$

5 $CONFER_{exec}(Bob, Charlie, Process1)$

6 $TRANSFER_{exec}(Alice, Charlie, Process1)$

7 $CONFER_{*write}(Charlie, Bob, File1)$

8 $REVOKE_{read}(Bob, Charlie, File2)$

9 $REVOKE_{read}(Alice, Alice, File1)$

10 $TRANSFER_{read}(Alice, David, File1)$

11 $REVOKE_{read}(Charlie, David, File1)$

12 $CREATE(Charlie, File3)$

13 $CONFER_{*read}(Charlie, Bob, File3)$

14 $TRANSFER_{read}(Bob, Alice, File3)$

15 $TRANSFER_{read}(Charlie, Bob, File2)$

16 $REVOKE_{read}(Charlie, Bob, File3)$

17 $TRANSFER_{read}(Charlie, David, File2)$

18 $REVOKE_{read}(Bob, David, File2)$

19 $CONFER_{*read}(Bob, Charlie, File2)$

20 $TRANSFER_{write}(Charlie, Alice, File1)$

Hints:

- Command $CONFER_{*read}$ is equal to $CONFER_{read}$ but grants $*read$ instead of $read$. Similar principle applies to $CONFER_{*exec}$ and $CONFER_{*write}$.
- Command $REVOKE_{read}$ removes both $read$ and $*read$. Similar principle applies to $REVOKE_{exec}$ and $REVOKE_{write}$.

(b) Is α leaking access privileges? (Consider only David to be untrusted) Justify the answer.

Solution (a) The final access control metrics is:

	File 1	File 2	File 3	Process 1
Alice	*read (1) write (3)		read (14)	exec (2)
Bob	*write (7)	own (0) read (4)	~~read~~ (13) (16)	own (0)
Charlie	own (0)	~~*read~~ (8) *read (19)	own (12)	exec (5)
David	~~read~~ (10) (11)			

The command whose execution leads to the right is listed in parenthesis.

The other commands:

6 cannot be executed because Alice does not have the delegation right (*) for exec on Process 1.

9 cannot be executed because Alice is not the owner of File 1.

15 cannot be executed because Charlie does not have read right with the delegation right (*) on File 2 at this point of the execution.

17 cannot be executed because Charlie does not have read right with the delegation right (*) on File 2 at this point of the execution.

18 is executed but it has no effect.

20 cannot be executed because Charlie does not have write right with the delegation right (*) on File 1.

Solution (b) Yes, the sequence of commands leaks access privileges as, at a certain point of the execution, David has read right on File 1.

Q2. Let TOP SECRET, SECRET, CONFIDENTIAL and UNCLASSIFIED be the integrity levels (ordered from highest to lowest), and Navy and Army two categories. Consider the following subjects and objects along with their integrity classes:

Subject	**Integrity Class**
President	(TOP SECRET,{Army,Navy})
Colonel	(SECRET,{Army})
Major	(CONFIDENTIAL,{Navy})
Soldier	(UNCLASSIFIED,{Army,Navy})

Object	**Integrity Class**
Army position	(SECRET,{Army})
Fleet position	(SECRET,{Navy})
Number of army units	(CONFIDENTIAL,{Army})
Number of navy units	(CONFIDENTIAL,{Navy})
Cost of army unit	(UNCLASSIFIED,{Army})
Cost of navy unit	(UNCLASSIFIED,{Navy})

Answer the following questions based on the Biba model:

(a) Can the president compute the overall defense costs (army + navy)?
(b) Can the major compute the cost per army unit?
(c) Can the soldier compute the cost per navy unit?
(d) Can the colonel change the overall defense position?
(e) Can the major change the cost of navy and army units?
(f) Can the soldier change the fleet

position? Justify the answers.

Hint:

- Changing an object requires 'write' rights over the object.
- Computing requires 'read' rights over the (input) objects.

Solution (b) Can the president compute the overall defense costs (army + navy)?

Clearance President: $(TOP\ SECRET, \{Army, Navy\})$
Classification Cost of army unit: $(UNCLASSIFIED, \{Army\})$
Classification Cost of navy unit: $(UNCLASSIFIED, \{Navy\})$

$$(TOP\ SECRET, \{Army, Navy\}) \not\leq (UNCLASSIFIED, \{Army\})$$
$$(TOP\ SECRET, \{Army, Navy\}) \not\leq (UNCLASSIFIED, \{Navy\})$$

However, if the president sets his/her current security class at $(UNCLASSIFIED, \{\})$:

$$(UNCLASSIFIED, \{\}) \leq (UNCLASSIFIED, \{Army\})$$
$$(UNCLASSIFIED, \{\}) \leq (UNCLASSIFIED, \{Navy\})$$

The president can compute the overall defense costs but only if he/she accesses the system at a lower security class.

Solution (c) Can the major compute the cost per army unit?

Clearance Major: $(CONFIDENTIAL, \{Navy\})$
Classification Cost of army unit: $(UNCLASSIFIED, \{Army\})$

Classification Number of army units: $(CONFIDENTIAL, \{Army\})$

$(CONFIDENTIAL, \{Navy\}) \not\leq (UNCLASSIFIED, \{Army\})$
$(CONFIDENTIAL, \{Navy\}) \not\leq (CONFIDENTIAL, \{Army\})$

However, if the major sets his/her current security class at $(UNCLASSIFIED, \{\})$:

$(UNCLASSIFIED, \{\}) \leq (UNCLASSIFIED, \{Army\})$
$(UNCLASSIFIED, \{\}) \leq (CONFIDENTIAL, \{Army\})$

Therefore, the major can compute the cost per army unit but only if he/she accesses the system at a lower security class.

Solution (d) Can the soldier compute the cost per navy unit?

Clearance Soldier: $(UNCLASSIFIED, \{Army, Navy\})$
Classification Cost of navy unit: $(UNCLASSIFIED, \{Navy\})$
Classification Number of navy units: $(CONFIDENTIAL, \{Navy\})$

$(UNCLASSIFIED, \{Army, Navy\}) \not\leq (UNCLASSIFIED, \{Navy\})$
$(UNCLASSIFIED, \{Army, Navy\}) \not\leq (CONFIDENTIAL, \{Navy\})$

However, if the soldier sets his/her current security class at $(UNCLASSIFIED, \{Navy\})$:

$(UNCLASSIFIED, \{Navy\}) \leq (UNCLASSIFIED, \{Navy\})$
$(UNCLASSIFIED, \{Navy\}) \leq (CONFIDENTIAL, \{Navy\})$

Therefore, the soldier can compute the cost per navy unit but only if he/she accesses the system at a lower security class.

Solution (e) Can the colonel change the overall defense position?

Clearance Colonel: $(SECRET, \{Army\})$
Classification Army position: $(SECRET, \{Army\})$
Classification Fleet position: $(SECRET, \{Navy\})$

$(SECRET, \{Army\}) \geq (SECRET, \{Army\})$
$(SECRET, \{Army\}) \not\geq (SECRET, \{Navy\})$

The colonel can change the army position but not the fleet position.

Solution (f) Can the major change the cost of navy and army units?

Clearance Major: $(CONFIDENTIAL, \{Navy\})$

Classification Cost of army unit: $(UNCLASSIFIED, \{Army\})$
Classification Cost of navy unit: $(UNCLASSIFIED, \{Navy\})$

$(CONFIDENTIAL, \{Navy\}) \not\geq (UNCLASSIFIED, \{Army\})$
$(CONFIDENTIAL, \{Navy\}) \geq (UNCLASSIFIED, \{Navy\})$

The major can change the cost of navy units but not the cost of army units.

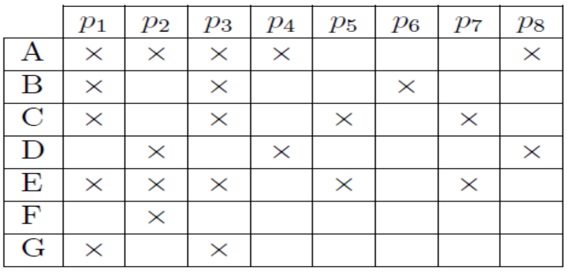
Solution (g) Can the soldier change the fleet position?

Clearance Soldier: $(UNCLASSIFIED, \{Army, Navy\})$
Classification Fleet position: $(SECRET, \{Navy\})$

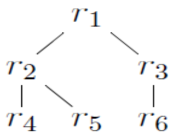
$(UNCLASSIFIED, \{Army, Navy\}) \not\geq (SECRET, \{Navy\})$

No, the soldier cannot change the fleet position.

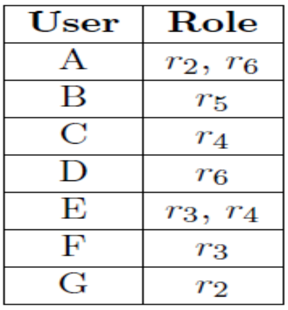
Q3. The following access matrix has been generate from an RBAC$_1$ policy with the given hierarchy and where C has role r_4. Give the minimal User-Assignment and Permission- Assignment corresponding to the given Access Matrix such that you do not assign anything that can be already derived otherwise.



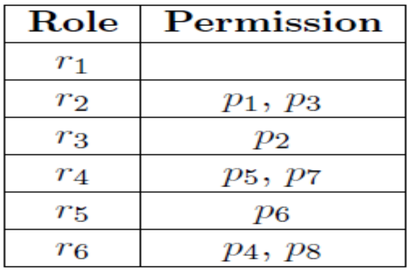
	p_1	p_2	p_3	p_4	p_5	p_6	p_7	p_8
A	×	×	×	×				×
B	×		×			×		
C	×		×		×		×	
D		×		×				×
E	×	×	×		×		×	
F		×						
G	×		×					



Hint: Users might have more than one role
Solution:



User	Role
A	r_2, r_6
B	r_5
C	r_4
D	r_6
E	r_3, r_4
F	r_3
G	r_2



Role	Permission
r_1	
r_2	p_1, p_3
r_3	p_2
r_4	p_5, p_7
r_5	p_6
r_6	p_4, p_8