EXAM SOLUTIONS

Principles of Data Protection

November 17, 2023

Contents

1 Discretionary Access Control **1**

1.1 Exam 23/1/2017: Question 1 1

1.2 Exam 22/1/2018: Question 1 3

1.3 Exam 2/11/2018: Question 1 5

2 Mandatory Access Control **7**

2.1 Biba model 7

2.1.1 Exam 31/1/2013: Question 2 7

2.2 Biba model with low-watermark for subjects 11

2.2.1 Exam 30/10/2017: Question 2 11

2.2.2 Exam 25/1/2019: Question 1 14

2.2.3 Exam 30/10/2020: Part A Question 1 18

3 Role-Based Access Control **22**

3.1 Exam 30/10/2017: Question 3 22

3.2 Exam 25/1/2019: Question 2 24

3.3 Exam 24/1/2020: Question 2 25

4 RT **26**

4.1 Exam 30/10/2017: Question 4(a) 26

4.2 Exam 25/1/2019: Question 3(a) 28

4.3 Exam 24/1/2020: Question 3(b) 30

4.4 Exam 18/1/2021: Part A Question 2(b) 32

5 UCON **34**

5.1 Exam 27/1/2016: Question 4 34

6 Privacy-aware Access Control **36**
6.1 Purpose-based Access Control 36
6.1.1 Exam 31/1/2013: Question 5 36
6.2 EPAL (Policy evaluation) 38
6.2.1 Exam 22/1/2018: Question 5 38
6.2.2 Exam 2/11/2018: Question 5 39
6.2.3 Exam 30/10/2020: Part B Question 2 40
6.3 EPAL (Policy refinement) 41
6.3.1 Exam 29/1/2014: Question 6 41

7 Decision Reduction **44**
7.1 Exam 27/1/2016: Question 5(a,c) 44
7.2 Exam 25/1/2019: Question 5(a,c) 46
7.3 Exam 1/11/2019: Question 5(a,c) 47

8 XACML **48**
8.1 Exam 30/10/2017: Question 6 48
8.2 Exam 22/1/2018: Question 6 55
8.3 Exam 2/11/2018: Question 6 63
8.4 Exam 25/1/2019: Question 6 70
8.5 Exam 1/11/2019: Question 6 77
8.6 Exam 24/1/2020: Question 6 84
8.7 Exam 18/1/2021: Part B Question 3 91

Chapter 1

Discretionary Access Control

1.1 Exam 23/1/2017: Question 1

Consider a protection system with the following commands:

command create_file(s, o)
  create object o
  enter own into $A[s, o]$ **end**.

command confer_itself(s, o, r)
  if own into $A[s, o]$
  then enter r into $A[s, o]$ **end**.

command confer_others(s_1, s_2, o, r)
  if own into $A[s_1, o]$ and
    $r \neq$ write
  then enter r into $A[s_2, o]$ **end**.

command transfer_rights(s_1, s_2, o, r)
  if exec into $A[s_1, o]$
  then enter r into $A[s_2, o]$ **end**.

(Right own cannot be conferred and/or transfered.)

Suppose Bob wants to share some documents with other users. Users should be able to read those documents, but they cannot modify them (consider right write for modification). Is the system secure? Justify the answer.

Solution A system is secure with respect to a right r if there does not exist any sequence of commands leaking r. Consider the following sequence of commands:

create_file(Bob,newfile)
confer_others(Bob,Alice,newfile,exec)
transfer_rights(Alice,Alice,newfile,write)

After executing these commands, Alice has right write on newfile. Therefore, the system is NOT secure.

1.2 Exam 22/1/2018: Question 1

Recall the HUR model.

(a) 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.

1.3 Exam 2/11/2018: Question 1

Recall the HUR model.

(a) Compute the access matrix that results from the following initial state

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

by executing the sequence of commands α defined as follows:

1 $CONFER_{*exec}(Bob, Alice, Process1)$
2 $CONFER_{read}(Alice, Charlie, File1)$
3 $CONFER_{*write}(Alice, Bob, File1)$
4 $CONFER_{*write}(Alice, Bob, File2)$
5 $TRANSFER_{write}(Bob, Charlie, File1)$
6 $TRANSFER_{read}(Charlie, Bob, File1)$
7 $TRANSFER_{read}(Alice, Charlie, File1)$
8 $TRANSFER_{write}(Bob, David, File2)$
9 $REVOKE_{read}(Charlie, Alice, File2)$
10 $CONFER_{write}(Charlie, Bob, File2)$
11 $TRANSFER_{read}(Alice, David, File2)$
12 $CREATE(Charlie, Process1)$
13 $CONFER_{*exec}(Charlie, Alice, Process1)$
14 $TRANSFER_{exec}(Alice, David, Process1)$
15 $REVOKE_{exec}(Charlie, David, File2)$
16 $CREATE(Charlie, Process2)$
17 $TRANSFER_{exec}(Charlie, David, Process2)$
18 $TRANSFER_{exec}(Charlie, Alice, Process2)$
19 $REVOKE_{read}(Charlie, Bob, File2)$
20 $REVOKE_{exec}(Charlie, David, Process2)$

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	Process 1	Process 2
Alice	own (0)		*exec (1)	
Bob	*write (3)	~~*read~~ (19) write (10)	own (0)	
Charlie	read (2) write (5)	own (0)		own (16)
David			exec (14)	

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

The other commands:

4 cannot be executed because Alice is not the owner of File 2.
6 cannot be executed because Charlie does not have the delegation right (*) for read on File 1.
7 cannot be executed because Alice does not have the delegation right (*) for read on File 1.
8 cannot be executed because Bob does not have the delegation right (*) for write on File 2.
9 is executed but it has no effect.
11 cannot be executed because Alice does not have read right with the delegation right (*) on File 2.
12 cannot be executed because Process 1 already exists.
13 cannot be executed because Charlie is not the owner of Process 1.
15 is executed but it has no effect.
17 cannot be executed because Charlie does not have exec right with the delegation right (*) on Process 2.
18 cannot be executed because Charlie does not have exec right with the delegation right (*) on Process 2.
20 is executed but it has no effect.

Solution (b) Yes, the sequence of commands leaks access privileges as David has the right to execute Process 1.

Chapter 2

Mandatory Access Control

2.1 Biba model

2.1.1 Exam 31/1/2013: Question 2

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:

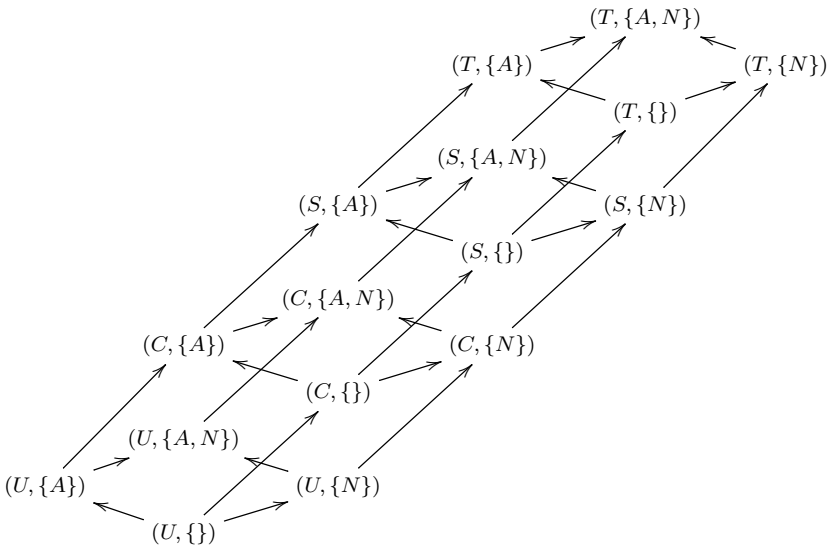
(a) Draw the lattice of classifications.
(b) Can the president compute the overall defense costs (army + navy)?
(c) Can the major compute the cost per army unit?
(d) Can the soldier compute the cost per navy unit?
(e) Can the colonel change the overall defense position?
(f) Can the major change the cost of navy and army units?
(g) 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 (a) Lattice of classification:



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.

2.2 Biba model with low-watermark for subjects

2.2.1 Exam 30/10/2017: Question 2

Let HIGH, MEDIUM and LOW be integrity levels (ordered from the highest to the lowest). Let Navy and Army be two categories. Consider the following subjects and objects along with their integrity classes:

Subject	**Integrity**
Colonel	(HIGH,{Navy})
Major	(MEDIUM,{Army})
Captain	(MEDIUM,{Army,Navy})
Soldier	(LOW,{Army,Navy})

Object	**Integrity**
Army position	(HIGH,{Army})
Fleet position	(HIGH,{Navy})
Number of army units	(MEDIUM,{Army})
Number of navy units	(MEDIUM,{Navy})
Cost of army units	(LOW,{Army})
Cost of navy units	(LOW,{Navy})

Answer the following questions based on the Biba model with low-watermark for subjects:

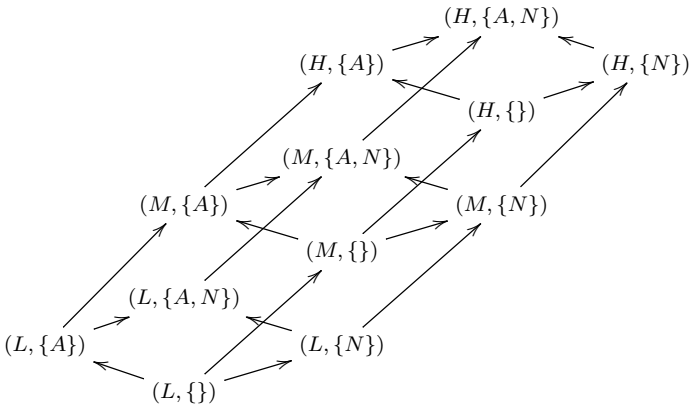
(a) Draw the lattice of classifications.
(b) Can the colonel change the number of navy units?
(c) Can the colonel change the number of navy units, after he read the cost of navy units?
(d) Can the major change the number of army units, after the colonel read it?
(e) Can the major change the cost of army units, after he read the fleet position?
(f) Can the captain compute the cost of the overall defense (i.e., army and navy) units?
(g) Can the soldier read the number of navy units, after he modified it?

Justify your answer.

Hint:

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

Solution (a) Lattice of classification:



Solution (b) Can the colonel change the Number of navy units?

Integrity Class Colonel: $(HIGH, \{Navy\})$
Integrity Class Number of navy units: $(MEDIUM, \{Navy\})$

$(HIGH, \{Navy\}) \geq (MEDIUM, \{Navy\})$

Yes, the colonel can change the number of army units.

Solution (c) Can the colonel change the number of navy units, after he read the cost of navy units?

Integrity Class Colonel: $(HIGH, \{Navy\})$
Integrity Class Number of navy units: $(MEDIUM, \{Navy\})$
Integrity Class Cost of navy units: $(LOW, \{Navy\})$

After the colonel read the cost of navy units:

$\lambda(Colonel) = glb((HIGH, \{Navy\}), (LOW, \{Navy\})) = (LOW, \{Navy\})$

$(LOW, \{Navy\}) \ngeq (MEDIUM, \{Navy\})$

No, the colonel can change the number of navy units after he read the cost of navy units.

Solution (d) Can the major change the number of army units, after the colonel read it?

Integrity Class Major: $(MEDIUM, \{Army\})$
Integrity Class Number of army units: $(MEDIUM, \{Army\})$

$MEDIUM, \{Army\}) \geq (MEDIUM, \{Army\})$

Yes, the colonel can change the number of army units. Note that having the colonel reading the number of army units does not change the integrity class of the object.

Solution (e) Can the major change the cost of army units, after he read the fleet position?

Integrity Class Major: $(MEDIUM, \{Army\})$
Integrity Class Cost of army units: $(LOW, \{Army\})$
Integrity Class Fleet position: $(HIGH, \{Navy\})$

After the major read the fleet position:

$$\lambda(Major) = glb((MEDIUM, \{Army\}), (HIGH, \{Navy\})) = (MEDIUM, \{\})$$

$$(MEDIUM, \{\}) \not\geq (LOW, \{Army\})$$

No, the major cannot change the cost of army units after he read the fleet position.

Solution (f) Can the captain compute the cost of the overall defense (i.e., army and navy) units?

Read operations are always allowed by the Biba model with low-watermarking for subjects. After reading the captain's integrity class changes to $(LOW, \{\})$.

Solution (g) Can the soldier read the number of navy units, after he modified it?

Read operations are always allowed by the Biba model with low-watermarking for subjects. After reading the soldier's integrity class changes to $(LOW, \{Navy\})$. Also, note that having the soldier modifying the number of navy units does not change the his integrity class nor the one of the object.

2.2.2 Exam 25/1/2019: Question 1

Let HIGH, MEDIUM and LOW be integrity levels (ordered from the highest to the lowest). Let Navy and Army be two categories. Consider the following subjects and objects along with their integrity classes:

Subject	**Integrity**
Colonel	(HIGH,{Army,Navy})
Major	(MEDIUM,{Army,Navy})
Captain	(MEDIUM,{Navy})
Soldier	(LOW,{Army})

Object	**Integrity**
Army position	(HIGH,{Army})
Fleet position	(HIGH,{Navy})
Number of army units	(MEDIUM,{Army})
Number of navy units	(MEDIUM,{Navy})
Cost of army units	(LOW,{Army})
Cost of navy units	(LOW,{Navy})

Answer the following questions based on the Biba model with low-watermark for subjects:

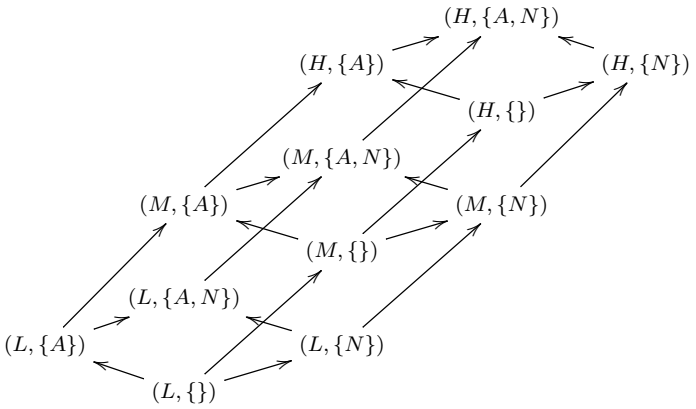
(a) Draw the lattice of classifications.
(b) Can the colonel change the cost of army units?
(c) Can the colonel change the cost of army units, after he read the fleet position?
(d) Can the major compute the overall cost of defense (i.e., army and navy) units?
(e) Can the captain change the cost of army units, after he read the fleet position?
(f) Can the captain change the number of navy units, after the soldier read it?
(g) Can the soldier change the cost of army units, after he read the cost of navy units?

Justify your answer.

Hint:

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

Solution (a) Lattice of classification:



Solution (b) Can the colonel change the cost of army units?

Integrity Class Colonel: $(HIGH, \{Army, Navy\})$
Integrity Class Cost of army units: $(LOW, \{Army\})$

$(HIGH, \{Army, Navy\}) \geq (LOW, \{Army\})$

Yes, the colonel can change the cost of army units.

Solution (c) Can the colonel change the cost of army units, after he read the fleet position?

Integrity Class Colonel: $(HIGH, \{Army, Navy\})$
Integrity Class Cost of army units: $(LOW, \{Army\})$
Integrity Class Fleet position: $(HIGH, \{Navy\})$

After the colonel read the fleet position:

$\lambda(Colonel) = glb((HIGH, \{Army, Navy\}), (HIGH, \{Navy\})) = (HIGH, \{Navy\})$

$(HIGH, \{Navy\}) \not\geq (LOW, \{Army\})$

No, the colonel cannot change the cost of army units after he read the fleet position.

Solution (d) Can the major compute the overall cost of defense (i.e., army and navy) units?

Integrity Class Major: $(MEDIUM, \{Army, Navy\})$
Integrity Class Cost of army units: $(LOW, \{Army\})$

Integrity Class Cost of navy units: $(LOW, \{Navy\})$

Read operations are always allowed by the Biba model with low-watermarking for subjects. After reading the major's integrity class changes to $(LOW, \{\})$.

Solution (e) Can the captain change the cost of army units, after he read the fleet position?

Integrity Class Captain: $(MEDIUM, \{Navy\})$
Integrity Class Cost of army units: $(LOW, \{Army\})$
Integrity Class Fleet position: $(HIGH, \{Navy\})$

After the captain read the fleet position:

$$\lambda(Captain) = glb((MEDIUM, \{Navy\}), (HIGH, \{Navy\})) = (MEDIUM, \{Navy\})$$

$$(MEDIUM, \{Navy\}) \not\geq (LOW, \{Army\})$$

No, the colonel cannot change the cost of army units after he read the fleet position.

Solution (f) Can the captain change the number of navy units, after the soldier read it?

Integrity Class Captain: $(MEDIUM, \{Navy\})$
Integrity Class Number of navy units: $(LOW, \{Navy\})$
Integrity Class Fleet position: $(HIGH, \{Navy\})$

$$(MEDIUM, \{Navy\}) \geq (LOW, \{Navy\})$$

Yes, the captain can change the number of navy units. Note that having the soldier reading the number of navy units does not change the integrity class of the object.

Solution (g) Can the soldier change the cost of army units, after he read the cost of navy units?

Integrity Class Soldier: $(LOW, \{Army\})$
Integrity Class Cost of army units: $(LOW, \{Army\})$
Integrity Class Cost of navy units: $(LOW, \{Navy\})$

After the soldier read the cost of navy units:

$$\lambda(Soldier) = glb((LOW, \{Army\}), (LOW, \{Navy\})) = (LOW, \{\})$$

$$(LOW, \{\}) \not\geq (LOW, \{Army\})$$

No, the soldier cannot change the cost of army units after he read the cost of navy units.

2.2.3 Exam 30/10/2020: Part A Question 1

Let HIGH, MEDIUM and LOW be integrity levels (ordered from the highest to the lowest). Let Navy and Army be two categories. Consider the following subjects and objects along with their integrity classes:

Subject	**Integrity**
Colonel	(HIGH,{Navy})
Major	(MEDIUM,{Army})
Captain	(MEDIUM,{Army, Navy})
Soldier	(LOW,{Army})

Object	**Integrity**
Army position	(HIGH,{Army})
Fleet position	(HIGH,{Navy})
Number of army units	(MEDIUM,{Army})
Number of navy units	(MEDIUM,{Navy})
Cost of army units	(LOW,{Army})
Cost of navy units	(LOW,{Navy})

Answer the following questions based on the Biba model with low-watermark for subjects:

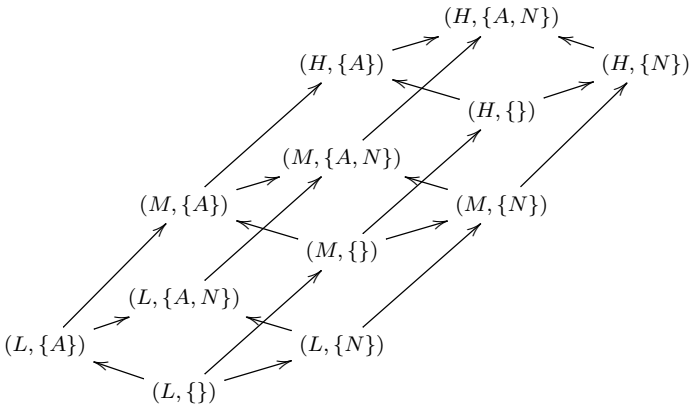
1. Draw the lattice of classifications.
2. Can the colonel read the number of army units?
3. Can the colonel change the fleet position, after he read the number of army units?
4. Can the major change the number of navy units, after the captain read it?
5. Can the captain change the cost of navy units, after he read the army position?
6. Can the captain change the cost of the overall defense (i.e., army and navy) units?
7. Can the soldier read the army position, after he modified it?

Justify your answer.

Hint:

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

Solution (a) Lattice of classification:



Solution (b) Can the colonel read the number of army units?

Integrity Class Colonel: $(HIGH, \{Navy\})$
Integrity Class Number of army units: $(MEDIUM, \{Army\})$

Read operations are always allowed by the Biba model with low-watermarking for subjects.

After reading the colonel's integrity class changes to:

$$\lambda(Colonel) = glb((HIGH, \{Navy\}), (MEDIUM, \{Navy\})) = (MEDIUM, \{\})$$

Solution (c) Can the colonel change the fleet position, after he read the number of army units?

Integrity Class Colonel: $(HIGH, \{Navy\})$
Integrity Class Fleet position: $(HIGH, \{Navy\})$
Integrity Class Number of army units: $(MEDIUM, \{Army\})$

After the colonel read the number of army units:

$$\lambda(Colonel) = glb((HIGH, \{Navy\}), (MEDIUM, \{ArmyNavy\})) = (MEDIUM, \{\})$$

$$(MEDIUM, \{\}) \not\geq (HIGH, \{Navy\})$$

No, the colonel cannot change the fleet position after he read the number of army units.

Solution (d) Can the major change the number of navy units, after the captain read it?

Integrity Class Major: $(MEDIUM, \{Army\})$

Integrity Class Number of navy units: $(MEDIUM, \{Navy\})$
Integrity Class Captain: $(MEDIUM, \{Army, Navy\})$

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

No, the colonel cannot change the number of navy units.

Note that the captain reading the number of navy units does not change the integrity class of the major or of the number of navy units.

Solution (e) Can the captain change the cost of navy units, after he read the army position?

Integrity Class Captain: $(MEDIUM, \{Army, Navy\})$
Integrity Class Cost of navy units: $(LOW, \{Navy\})$
Integrity Class Army position: $(HIGH, \{Army\})$

After the captain read the army position:

$\lambda(CAPTAIN) = glb((MEDIUM, \{Army, Navy\}), ((HIGH, \{Army\})) = (MEDIUM, \{Army\})$

$(MEDIUM, \{Army\}) \not\geq (LOW, \{Navy\})$

No, the captain cannot change the cost of navy units, after he read the army position.

Solution (f) Can the captain change the cost of the overall defense (i.e., army and navy) units?

Integrity Class Captain: $(MEDIUM, \{Army, Navy\})$
Integrity Class Cost of army units: $(LOW, \{Army\})$
Integrity Class Cost of navy units: $(LOW, \{Navy\})$

$(MEDIUM, \{Army, Navy\}) \geq (LOW, \{Army\})$
$(MEDIUM, \{Army, Navy\}) \geq (LOW, \{Navy\})$

Yes, the captain can change the cost of the overall defense units.

Solution (g) Can the soldier read the army position, after he modified it?

Integrity Class Soldier: $(LOW, \{Army\})$
Integrity Class Army position: $(HIGH, \{Army\})$

Read operations are always allowed by the Biba model with low-watermarking for subjects.

After reading the soldier's integrity class changes to:

$$\lambda(Soldier) = glb((LOW, \{Army\}), (HIGH, \{Army\})) = (LOW, \{Army\})$$

Note that the soldier cannot modify the army position ($(LOW, \{Army\}) \not\geq (HIGH, \{Army\})$).

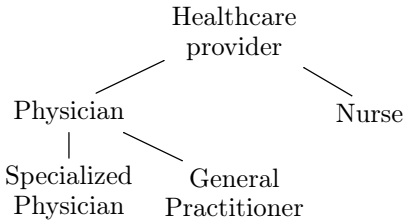
Chapter 3

Role-Based Access Control

3.1 Exam 30/10/2017: Question 3

The following Access Matrix has been generate from an RBAC_1 policy with the given hierarchy and where Bob has role "Physician". 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.

	Prescription	Medical History	Scan
Alice	read, write	read	read, insert
Bob	read	read	read
Charlie	read	write	
David	read	read	read, insert
Eve	read, write	read	read
Frank	read, write	read, write	read
Gill	read	read, write	read, insert



Solution

Permission Assignment

Healthcare provider	(read,prescription)
Physician	(read,medical_history)
	(read,scan)
Specialized physician	(insert,scan)
General practitioner	(write,prescription)
Nurse	(write,medical_history)

User Assignment

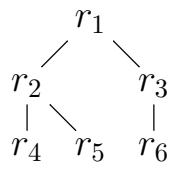
Alice	General practitioner
	Specialized physician
Bob	Physician
Charlie	Nurse
David	Specialized physician
Eve	General practitioner
Frank	General practitioner
	Nurse
Gill	Specialized physician
	Nurse

Note: The problem admits two solutions. The other solution is similar, where 'Specialized physician' and 'General practitioner' are inverted.

3.2 Exam 25/1/2019: Question 2

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

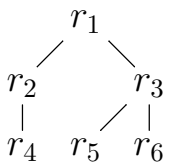
User	**Role**
A	r_2, r_6
B	r_5
C	r_4
D	r_6
E	r_3, r_4
F	r_3
G	r_2

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

3.3 Exam 24/1/2020: Question 2

The following access matrix has been generate from an RBAC_1 policy with the given hierarchy and where A has role r_6. 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_6
B	r_2
C	r_5
D	r_2, r_3
E	r_4
F	r_3
G	r_4, r_6

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

Chapter 4

RT

4.1 Exam 30/10/2017: Question 4(a)

Consider the following RT_0 policy:

$A.s \longleftarrow A.t.u$

$A.t \longleftarrow B.s$

$B.s \longleftarrow B.t.u$

$B.t \longleftarrow C.r$

$C.r \longleftarrow A$

$C.r \longleftarrow B$

$C.u \longleftarrow J$

$B.u \longleftarrow A$

$B.u \longleftarrow D$

$B.u \longleftarrow E$

$A.u \longleftarrow A$

$D.u \longleftarrow F$

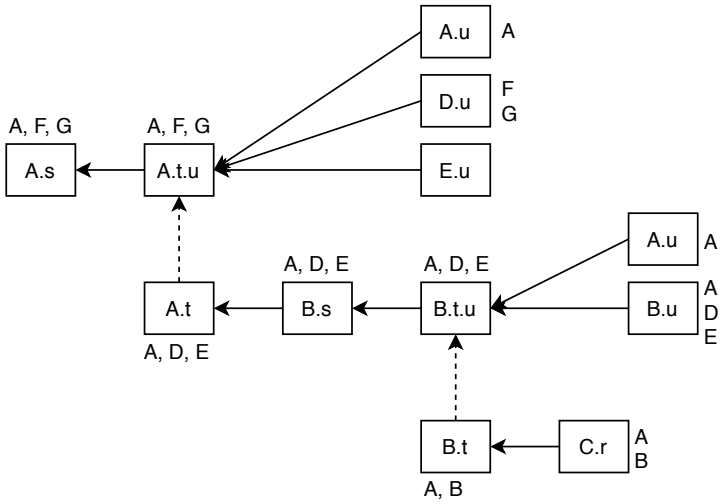
$D.u \longleftarrow G$

- Find all principals populating $A.s$ and $B.s$ (which means, compute $[\![A.s]\!]$ and $[\![B.s]\!]$).
- Write down the graph generated by the top-down algorithm when computing the semantics of $A.s$. (the top-down algorithm is also known as the "backward algorithm").

Solution

$[\![A.s]\!] = \{A, F, G\}$

$[\![B.s]\!] = \{A, D, E\}$



4.2 Exam 25/1/2019: Question 3(a)

Consider the following RT_0 policy.

$A.r \longleftarrow A.s.t$
$A.s \longleftarrow B.u \cap B.t$

$B.u \longleftarrow C$
$B.u \longleftarrow A.r$

$B.t \longleftarrow C.t$

$C.t \longleftarrow C$
$C.t \longleftarrow E$
$C.t \longleftarrow F$
$C.t \longleftarrow G$

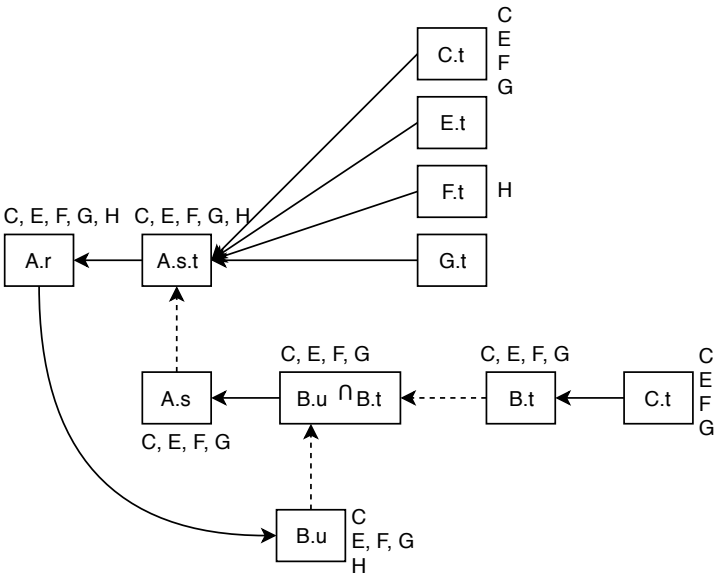
$F.t \longleftarrow H$

- Find all principals populating $A.s$ and $A.r$ (which means, compute $[\![A.s]\!]$ and $[\![A.r]\!]$).
- Write down the graph generated by the top-down algorithm when computing the semantics of $A.r$. (the top-down algorithm is also known as the "backward algorithm").

Solution

$[\![A.s]\!] = \{C, E, F, G\}$

$[\![A.r]\!] = \{C, E, F, G, H\}$



4.3 Exam 24/1/2020: Question 3(b)

Consider the following RT_0 policy.

$A.t \longleftarrow A.t.s$
$A.t \longleftarrow K.t$
$A.t \longleftarrow L.t$

$K.t \longleftarrow A.t$

$L.t \longleftarrow D$
$L.t \longleftarrow E$

$D.s \longleftarrow G$
$D.s \longleftarrow H$

$H.t \longleftarrow W$

$H.s \longleftarrow Z$

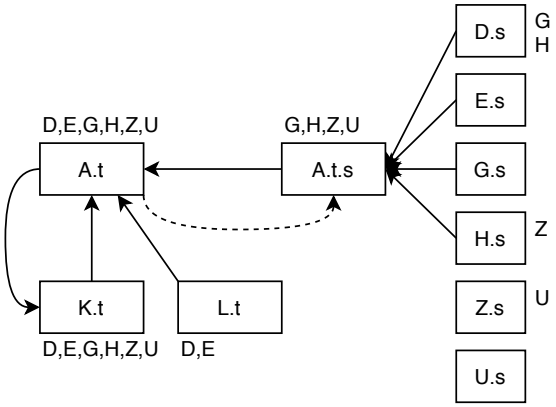
$Z.s \longleftarrow U$

$Z.t \longleftarrow R$

- Find all principals populating $A.t$ (which means, compute $[\![A.t]\!]$).
- Write down the graph generated by the top-down algorithm when computing the semantics of $A.t$. (the top-down algorithm is also known as the "backward algorithm").

Solution

$[\![A.t]\!] = \{D, E, G, H, Z, U\}$



4.4 Exam 18/1/2021: Part A Question 2(b)

Consider the following RT_0 policy.

$A.t \longleftarrow A.t.s$

$A.t \longleftarrow B$

$B.t \longleftarrow J$
$B.t \longleftarrow K$

$B.s \longleftarrow B.t.s$

$B.r \longleftarrow A$
$B.r \longleftarrow B$

$K.s \longleftarrow A$
$K.s \longleftarrow B$
$K.s \longleftarrow C$

$K.t \longleftarrow F$
$K.t \longleftarrow G$
$K.t \longleftarrow H$

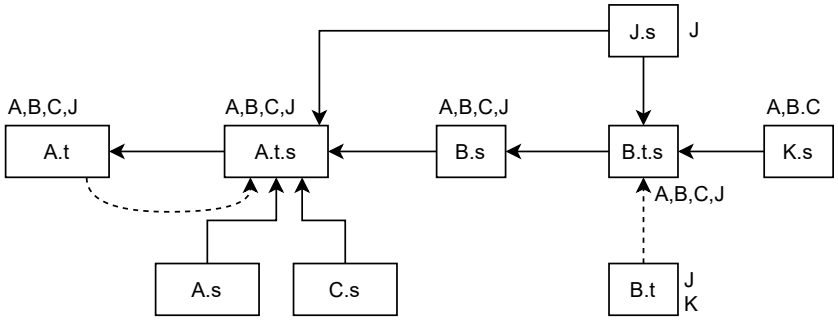
$K.v \longleftarrow L$
$K.v \longleftarrow M$
$K.v \longleftarrow N$

$J.s \longleftarrow J$

- Find all principals populating $A.t$ (which means, compute $[\![A.t]\!]$).
- Write down the graph generated by the top-down algorithm when computing the semantics of $A.t$. (the top-down algorithm is also known as the "backward algorithm").

Solution

$[\![A.t]\!] = \{A, B, C, J\}$



Chapter 5

UCON

5.1 Exam 27/1/2016: Question 4

Write a UCON policy supporting the following scenario.

A content provider offers an on-demand media streaming service. In order to access the service, users should subscribe to the service. The provider allows two types of subscription: Basic and Gold. Depending on the type of subscription, users can simultaneously connect a different number of devices to the provider's library of online content. In particular, the Basic subscription allows a user to connect one device whereas the Gold subscription allows a user to connect up to five devices. The service is offered only within Europe.

Solution
UCON Model: $UCON_{preA_{13}preB_1}$

- Pre Authorization ($preA$)
  - Access is only offered within Europe.
  - Constraint on the number of devices that a user can connect to.
- Pre Obligation ($preB$)
  - Subscription to the service.
- Update
  - Record whether a user is subscribed (and the type of subscription).
  - Record the number of devices currently connected.

UCON Policy

S: set of users
O: set of objects
IP: set of IPs
$IP_{EU} \subseteq IP$: set of IPs in EU
$SubType = \{Basic, Gold\}$ type of subscription

$location : S \to IP$
$subscription : S \nrightarrow SubType$ (partial function)
$ndevice : S \to \mathbb{N}$ number of devices a user has connected to the service

$ATT(s) : \{location, subscription, ndevice\}$
$ATT(o) : \{\}$

$OBS = S$
$OBO = \{service\}$
$OB = \{subscribe\text{-}Basic, subscribe\text{-}Gold\}$

$$getPreOBL(s,o,r) = \begin{cases} (s, service, subscribe\text{-}Basic) & \text{if } subscription(s) = \bot \\ & \text{and } s \text{ wants Basic subscription } (*) \\ (s, service, subscribe\text{-}Gold) & \text{if } subscription(s) = \bot \\ & \text{and } s \text{ wants Gold subscription } (**) \\ \emptyset & \text{if } subscription(s) \neq \bot \end{cases}$$

(symbol '$\bot$' indicates 'undefined')

$$\begin{aligned} allow(s,o,r) &\Rightarrow location(s) \in IP_{NL} \\ allow(s,o,r) &\Rightarrow preFulfilled(getPreOBL(s,o,r)) \\ allow(s,o,r) &\Rightarrow (subscription(s) = Basic \wedge ndevice(s) < 1) \vee \\ &\quad\ (subscription(s) = Gold \wedge ndevice(s) < 5) \end{aligned}$$

$preUpdate(subscription(s)) : subscription(s) = Basic\ (*)$
$preUpdate(subscription(s)) : subscription(s) = Gold\ (**)$
$preUpdate(ndevice(s)) : ndevice(s) = ndevice(s) + 1$
$postUpdate(ndevice(s)) : ndevice(s) = ndevice(s) - 1$

Chapter 6

Privacy-aware Access Control

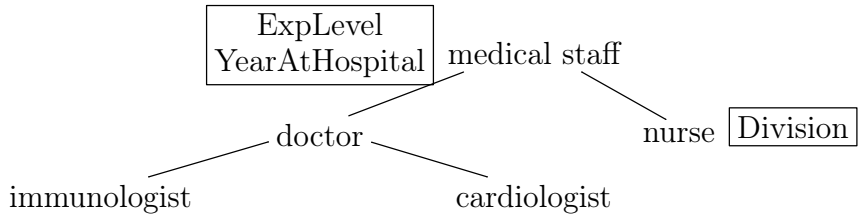
6.1 Purpose-based Access Control

6.1.1 Exam 31/1/2013: Question 5

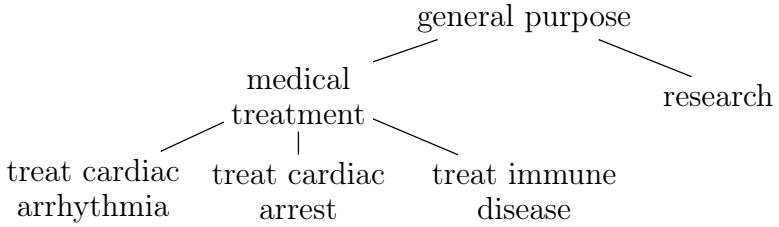
Define the purpose hierarchy, role hierarchy, and access purpose authorizations in Purpose-based Access Control for the following scenario.

Doctors are allowed to access patient information for providing medical treatment after they have worked for at least three years at the hospital. However, specialized doctors can access patient information for treating disease related to their specialization with one year experience at the hospital. For instance, cardiologists can treat cardiac arrhythmia and cardiac arrest, while immunologists can treat immune system related diseases. Nurses can access patient information for providing medical treatment. However, access is allowed only if the nurse has worked at the hospital for at least five years. Nurses in the cardiology division can access patient information for cardiac arrhythmia treatment with only two year experience at the hospital. Doctors with at least five year experience (at the hospital or in other research institutes) can access patient information for research purposes. Access to patient information for research purposes is allowed only within the hospital network.

Solution



(a) Role Hierarchy



(b) Purpose Hierarchy

Access Purpose Authorizations

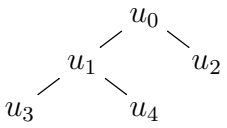
$\langle$medical treatment, $\langle$doctor, YearAtHospital $\geq 3\rangle\rangle$
$\langle$treat cardiac arrhythmia, $\langle$cardiologist, ExpLevel $\geq 1\rangle\rangle$
$\langle$treat cardiac arrest, $\langle$cardiologist, ExpLevel $\geq 1\rangle\rangle$
$\langle$treat immune disease, $\langle$immunologist, ExpLevel $\geq 1\rangle\rangle$
$\langle$medical treatment, $\langle$nurse, YearAtHospital $\geq 5\rangle\rangle$
$\langle$treat cardiac arrhythmia, $\langle$nurse, ExpLevel $\geq 2 \wedge$ Division = "*cardiology*"$\rangle\rangle$
$\langle$research, $\langle$doctor, ExpLevel $\geq 5 \wedge$ currIP $\in$ HospitalNetwork$\rangle\rangle$

6.2 EPAL (Policy evaluation)

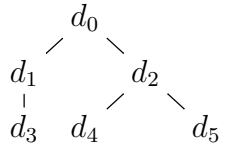
6.2.1 Exam 22/1/2018: Question 5

Let *pol* be an EPAL policy defined over a vocabulary *Voc* where *Voc* consists of the user, data, purpose and action hierarchies in Figure 6.2.

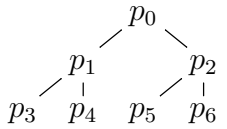
$$pol = \begin{cases} \langle (u_1, d_2, p_1, a_0)(\circ, true, o_1) \rangle \\ \langle (u_1, d_1, p_2, a_2)(+, true, o_2) \rangle \\ \langle (u_1, d_0, p_0, a_2)(\circ, true, o_3) \rangle \\ \langle (u_4, d_2, p_4, a_4)(-, true, o_4) \rangle \\ \langle (u_2, d_1, p_2, a_2)(+, true, o_5) \rangle \\ \text{Default ruling:} - \\ \text{Default obligations:} \{o_6\} \end{cases}$$



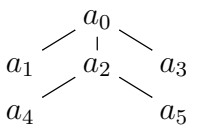
(a) User Hierarchy



(b) Data Hierarchy



(c) Purpose Hierarchy



(d) Action Hierarchy

Figure 6.2: Hierarchies

Evaluate the following access requests against *pol*:

$req_1 = (u_3, d_5, p_1, a_2)$
$req_2 = (u_4, d_3, p_6, a_3)$
$req_3 = (u_2, d_6, p_2, a_4)$
$req_4 = (u_2, d_3, p_6, a_5)$

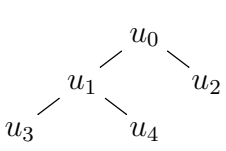
Solution

$req_1 : (-, \{o1, o3, o6\})$
$req_2 : (-, \{o6\})$
$req_3 : (scope\_error, \emptyset)$
$req_4 : (+, \{o5\})$

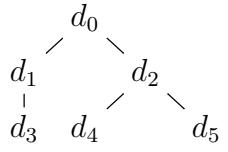
6.2.2 Exam 2/11/2018: Question 5

Let *pol* be an EPAL policy defined over the user hierarchy, data hierarchy, purpose hierarchy and action hierarchy in Figure 6.3.

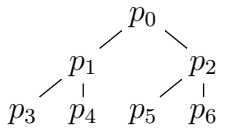
$$pol = \begin{cases} \langle (u_2, d_1, p_2, a_0)(\circ, true, o_1) \rangle \\ \langle (u_1, d_2, p_2, a_2)(+, true, o_2) \rangle \\ \langle (u_4, d_0, p_4, a_4)(-, true, o_3) \rangle \\ \langle (u_0, d_2, p_0, a_2)(\circ, true, o_4) \rangle \\ \langle (u_2, d_0, p_1, a_0)(-, true, o_5) \rangle \\ \text{Default ruling:}+ \\ \text{Default obligations:}\{o_6\} \end{cases}$$



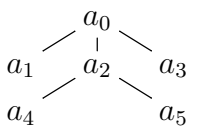
(a) User Hierarchy



(b) Data Hierarchy



(c) Purpose Hierarchy



(d) Action Hierarchy

Figure 6.3: Hierarchies

Evaluate the following access requests against *pol*:

$req_1 = (u_3, d_5, p_1, a_3)$
$req_2 = (u_2, d_4, p_4, a_4)$
$req_3 = (u_0, d_3, p_1, a_2)$
$req_4 = (u_2, d_3, p_3, a_2)$

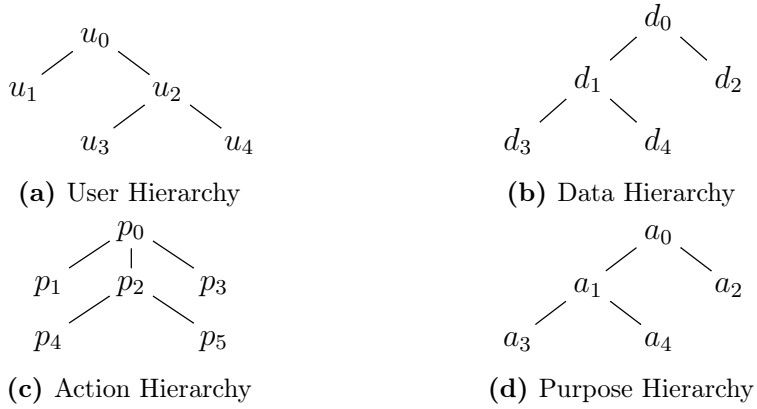
Solution

$req_1 : (+, \{o6\})$
$req_2 : (-, \{o4, o5\})$
$req_3 : (-, \{o3\})$
$req_4 : (-, \{o5\})$

6.2.3 Exam 30/10/2020: Part B Question 2

Let pol be an EPAL policy defined over the user hierarchy, data hierarchy, purpose hierarchy and action hierarchy in the figure below.

$$pol = \begin{cases} \langle (u_0, d_1, p_0, a_2)(+, true, \{o_1\}) \rangle \\ \langle (u_1, d_0, p_2, a_2)(-, true, \{o_2\}) \rangle \\ \langle (u_2, d_2, p_2, a_0)(\circ, true, \{o_3\}) \rangle \\ \langle (u_3, d_1, p_4, a_3)(-, true, \{o_4\}) \rangle \\ \langle (u_1, d_0, p_1, a_2)(+, true, \{o_5\}) \rangle \\ \text{Default ruling:} - \\ \text{Default obligations:} \{o_6\} \end{cases}$$



(a) User Hierarchy **(b)** Data Hierarchy

(c) Action Hierarchy **(d)** Purpose Hierarchy

Figure 6.4: Hierarchies

Evaluate the following access requests against *pol*:

$req_1 = (u_3, d_2, p_1, a_3)$
$req_2 = (u_2, d_4, p_2, a_0)$
$req_3 = (u_0, d_5, p_1, a_2)$
$req_4 = (u_2, d_2, p_4, a_3)$

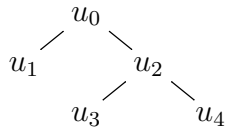
Solution

$req_1 : (-, \{o6\})$
$req_2 : (-, \{o4\})$
$req_3 : scope\_error$
$req_4 : (-, \{o3, o6\})$

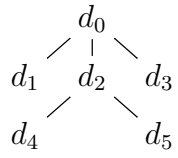
6.3 EPAL (Policy refinement)

6.3.1 Exam 29/1/2014: Question 6

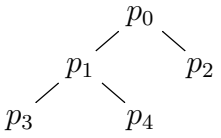
Let the hierarchies in Figure 6.5 be user hierarchy, data hierarchy, purpose hierarchy and action hierarchy. Let $(O, \rightarrow)$ be an obligation model with $O = \{o_1, o_2, o_3, o_4, o_5\}$ and $\rightarrow = \{o_1 \rightarrow o_2, o_1 \rightarrow o_3, o_4 \rightarrow o_5\}$.



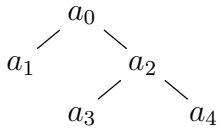
(a) User Hierarchy



(b) Data Hierarchy



(c) Purpose Hierarchy



(d) Action Hierarchy

Figure 6.5: Hierarchies

Consider the following EPAL policies:

$$pol_1 = \begin{cases} \langle (u_1, d_2, p_0, a_2)(+, true, \{o_1, o_4\}) \rangle \\ \langle (u_2, d_0, p_1, a_1)(\circ, true, \{o_4\}) \rangle \\ \langle (u_2, d_5, p_4, a_0)(-, true, \{o_1\}) \rangle \\ \langle (u_1, d_0, p_1, a_2)(+, true, \{o_5\}) \rangle \\ \text{Default ruling:}+ \\ \text{Default obligations:}\{o_2, o_4\} \end{cases}$$

$$pol_2 = \begin{cases} \langle (u_1, d_2, p_0, a_2)(+, true, \{o_2, o_4\}) \rangle \\ \langle (u_2, d_0, p_1, a_1)(\circ, true, \{o_4\}) \rangle \\ \langle (u_2, d_5, p_4, a_0)(-, true, \{o_1\}) \rangle \\ \langle (u_1, d_0, p_1, a_2)(+, true, \{o_5\}) \rangle \\ \langle (u_1, d_2, p_3, a_4)(+, true, \{o_1, o_4\}) \rangle \\ \text{Default ruling:}+ \\ \text{Default obligations:}\{o_2, o_4\} \end{cases}$$

$$pol_3 = \begin{cases} \langle (u_1, d_2, p_0, a_2)(+, true, \{o_1, o_4\}) \rangle \\ \langle (u_2, d_0, p_1, a_1)(\circ, true, \{o_4\}) \rangle \\ \langle (u_2, d_5, p_4, a_0)(-, true, \{o_1\}) \rangle \\ \langle (u_0, d_0, p_1, a_0)(+, true, \{o_1, o_4\}) \rangle \\ \langle (u_1, d_0, p_1, a_2)(+, true, \{o_5\}) \rangle \\ \langle (u_4, d_3, p_2, a_3)(-, true, \{o_3, o_4\}) \rangle \\ \text{Default ruling:}+ \\ \text{Default obligations:}\{o_2, o_4\} \end{cases}$$

Determine whether

(a) pol_2 is a refinement of pol_1,

(b) pol_3 is a refinement of pol_1.

Justify your answer.

Solution (a) Determine whether pol_2 is a refinement of pol_1:

- The first rule of pol_1 and pol_2 have the same scope but different obligations, where $\{o2\} \nrightarrow \{o1\}$.
- The fifth rule of pol_2 ($\langle(u_1, d_2, p_3, a_4)(+, true, \{o_1, o_4\})\rangle$) is not in pol_1. However, this rule will never be used as it is covered by the fourth rule of pol_2.

Consider request $req = (u_1, d_2, p_0, a_2)$.

- The evaluation of req against pol_1 yields $(+, \{o_1, o_4\})$.
- The evaluation of req against pol_2 yields $(+, \{o_2, o_4\})$.

Therefore, pol_2 is not a refinement of pol_1.

Solution (b) Determine whether pol_3 is a refinement of pol_1:

- The fourth rule of pol_3 ($\langle(u_0, d_0, p_1, a_0)(+, true, \{o_1, o_4\})$) is not in pol_1. This rule covers the fifth rule of pol_3 (which is the same of the forth rule of pol_1). The two rules have the same scope but different obligations. However, $\{o1, o4\}$ refines $\{o5\}$ because $o4 \rightarrow o5$. Moreover, the ruling is the same of the default ruling and the set of obligations ($\{o1, o4\}$) is a refinement of the default obligations because $o1 \rightarrow o2$.
- The sixth rule of pol_3 ($(u_4, d_3, p_2, a_3)(-, true, \{o_3, o_4\})$) is not in pol_1. This rule has a ruling different than the default ruling, which is the same in pol_1 and pol_3.

Consider request $req = (u_4, d_3, p_2, a_3)$.

- The evaluation of req against pol_1 yields $(+, \{o_2, o_4\})$.
- The evaluation of req against pol_3 yields $(-, \{o_3, o_4\})$.

Therefore, pol_3 is not a refinement of pol_1.

Chapter 7

Decision Reduction

7.1 Exam 27/1/2016: Question 5(a,c)

Consider an operator α defined over the three-valued decision set $\mathcal{D}_3 = \{1, 0, \bot\}$ defined as follows:

α	1	0	$\bot$
1	1	$\bot$	1
0	$\bot$	0	0
$\bot$	1	0	0

(a) Define α over a seven-valued decision set $\mathcal{D}_7$ point-wise (Recall $\mathcal{D}_7 = \wp(\mathcal{D}_3) \setminus \emptyset$).

(c) Let $\mathcal{D}_6 = \{P, D, NA, I(P), I(D), I(PD)\}$ be a six-valued decision set and $\rho_{76} : \mathcal{D}_7 \to \mathcal{D}_6$ a decision reduction that maps a decision in $\mathcal{D}_7$ to a decision in $\mathcal{D}_6$ such that

$$\rho_{76}(d) = \begin{cases} P & \text{if } d = 1 \quad I(P) \quad \text{if } d = \{1, \bot\} \\ D & \text{if } d = 0 \quad I(D) \quad \text{if } d = \{0, \bot\} \\ NA & \text{if } d = \bot \quad I(PD) \quad \text{if } d = \{1, 0\} \vee d = \{1, 0, \bot\} \end{cases}$$

Determine whether ρ_{76} is safe with respect to the operator α defined over $\mathcal{D}_7$.

Solution (a) The operator α over a seven-valued decision set $\mathcal{D}_7$ is defined as follows:

$\overline{\alpha}$	$\{1\}$	$\{0\}$	$\{\bot\}$	$\{1,\bot\}$	$\{0,\bot\}$	$\{1,0\}$	$\{1,0,\bot\}$
$\{1\}$	$\{1\}$	$\{\bot\}$	$\{1\}$	$\{1\}$	$\{1,\bot\}$	$\{1,\bot\}$	$\{1,\bot\}$
$\{0\}$	$\{\bot\}$	$\{0\}$	$\{0\}$	$\{0,\bot\}$	$\{0\}$	$\{0,\bot\}$	$\{0,\bot\}$
$\{\bot\}$	$\{1\}$	$\{0\}$	$\{0\}$	$\{1,0\}$	$\{0\}$	$\{1,0\}$	$\{1,0\}$
$\{1,\bot\}$	$\{1\}$	$\{0,\bot\}$	$\{1,0\}$	$\{1,0\}$	$\{1,0,\bot\}$	$\{1,0,\bot\}$	$\{1,0,\bot\}$
$\{0,\bot\}$	$\{1,\bot\}$	$\{0\}$	$\{0\}$	$\{1,0,\bot\}$	$\{0\}$	$\{1,0,\bot\}$	$\{1,0,\bot\}$
$\{1,0\}$	$\{1,\bot\}$	$\{0,\bot\}$	$\{1,0\}$	$\{1,0,\bot\}$	$\{1,0,\bot\}$	$\{1,0,\bot\}$	$\{1,0,\bot\}$
$\{1,0,\bot\}$	$\{1,\bot\}$	$\{0,\bot\}$	$\{1,0\}$	$\{1,0,\bot\}$	$\{1,0,\bot\}$	$\{1,0,\bot\}$	$\{1,0,\bot\}$

Solution (c) For every decision $d_1, d_2 \in \mathcal{D}_7$, we have that

$$\overline{\alpha}(\rho_{76}(d_1), \rho_{76}(d_2)) = \rho_{76}(\overline{\alpha}(d_1, d_2))$$

Therefore, the operator $\overline{\alpha}$ is safe with respect to ρ_{76}.

7.2 Exam 25/1/2019: Question 5(a,c)

Consider an operator α defined over the three-valued decision set $\mathcal{D}_3 = \{1, 0, \bot\}$ defined as follows:

α	1	0	$\bot$
1	0	$\bot$	0
0	$\bot$	1	1
$\bot$	0	1	$\bot$

(a) Define α over a seven-valued decision set $\mathcal{D}_7$ point-wise (Recall $\mathcal{D}_7 = \wp(\mathcal{D}_3) \setminus \emptyset$).

(c) Let $\mathcal{D}_6 = \{P, D, NA, I(P), I(D), I(PD)\}$ be a six-valued decision set and $\rho_{76} : \mathcal{D}_7 \to \mathcal{D}_6$ a decision reduction that maps a decision in $\mathcal{D}_7$ to a decision in $\mathcal{D}_6$ such that

$$\rho_{76}(d) = \begin{cases} P & \text{if } d = 1 \quad I(P) \quad \text{if } d = \{1, \bot\} \\ D & \text{if } d = 0 \quad I(D) \quad \text{if } d = \{0, \bot\} \\ NA & \text{if } d = \bot \quad I(PD) \quad \text{if } d = \{1, 0\} \vee d = \{1, 0, \bot\} \end{cases}$$

Determine whether ρ_{76} is safe with respect to the operator α defined over $\mathcal{D}_7$.

Solution (a) The operator α over a seven-valued decision set $\mathcal{D}_7$ is defined as follows:

$\overline{\alpha}$	$\{1\}$	$\{0\}$	$\{\bot\}$	$\{1, \bot\}$	$\{0, \bot\}$	$\{1, 0\}$	$\{1, 0, \bot\}$
$\{1\}$	$\{0\}$	$\{\bot\}$	$\{0\}$	$\{0\}$	$\{0, \bot\}$	$\{0, \bot\}$	$\{0, \bot\}$
$\{0\}$	$\{\bot\}$	$\{1\}$	$\{1\}$	$\{1, \bot\}$	$\{1\}$	$\{1, \bot\}$	$\{1, \bot\}$
$\{\bot\}$	$\{0\}$	$\{1\}$	$\{\bot\}$	$\{0, \bot\}$	$\{1, \bot\}$	$\{1, 0\}$	$\{1, 0, \bot\}$
$\{1, \bot\}$	$\{0\}$	$\{1, \bot\}$	$\{0, \bot\}$	$\{0, \bot\}$	$\{1, 0, \bot\}$	$\{1, 0, \bot\}$	$\{1, 0, \bot\}$
$\{0, \bot\}$	$\{0, \bot\}$	$\{1\}$	$\{1, \bot\}$	$\{1, 0, \bot\}$	$\{1, \bot\}$	$\{1, 0, \bot\}$	$\{1, 0, \bot\}$
$\{1, 0\}$	$\{0, \bot\}$	$\{1, \bot\}$	$\{1, 0\}$	$\{1, 0, \bot\}$	$\{1, 0, \bot\}$	$\{1, 0, \bot\}$	$\{1, 0, \bot\}$
$\{1, 0, \bot\}$	$\{0, \bot\}$	$\{1, \bot\}$	$\{1, 0, \bot\}$	$\{1, 0, \bot\}$	$\{1, 0, \bot\}$	$\{1, 0, \bot\}$	$\{1, 0, \bot\}$

Solution (c) For every decision $d_1, d_2 \in \mathcal{D}_7$, we have that

$$\overline{\alpha}(\rho_{76}(d_1), \rho_{76}(d_2)) = \rho_{76}(\overline{\alpha}(d_1, d_2))$$

Therefore, the operator $\overline{\alpha}$ is safe with respect to ρ_{76}.

7.3 Exam 1/11/2019: Question 5(a,c)

Consider an operator α defined over the three-valued decision set $\mathcal{D}_3 = \{1, 0, \bot\}$ defined as follows:

α	1	0	$\bot$
1	1	1	$\bot$
0	1	0	0
$\bot$	$\bot$	0	$\bot$

(a) Define α over the seven-valued decision set $\mathcal{D}_7$ in point-wise way (Recall $\mathcal{D}_7 = \wp(\mathcal{D}_3) \setminus \emptyset$).

(c) Let $\mathcal{D}_6 = \{P, D, NA, I(P), I(D), I(PD)\}$ be a six-valued decision set and $\rho_{76} : \mathcal{D}_7 \to \mathcal{D}_6$ a decision reduction that maps a decision in $\mathcal{D}_7$ to a decision in $\mathcal{D}_6$ such that:

$$\rho_{76}(d) = \begin{cases} P & \text{if } d = 1 \quad I(P) \quad \text{if } d = \{1, \bot\} \\ D & \text{if } d = 0 \quad I(D) \quad \text{if } d = \{0, \bot\} \\ NA & \text{if } d = \bot \quad I(PD) \quad \text{if } d = \{1, 0\} \vee d = \{1, 0, \bot\} \end{cases}$$

Determine whether ρ_{76} is safe with respect to the operator α defined over $\mathcal{D}_7$.

Solution (a) The operator α over a seven-valued decision set $\mathcal{D}_7$ is defined as follows:

$\overline{\alpha}$	$\{1\}$	$\{0\}$	$\{\bot\}$	$\{1, \bot\}$	$\{0, \bot\}$	$\{1, 0\}$	$\{1, 0, \bot\}$
$\{1\}$	$\{1\}$	$\{1\}$	$\{\bot\}$	$\{1, \bot\}$	$\{1, \bot\}$	$\{1\}$	$\{1, \bot\}$
$\{0\}$	$\{1\}$	$\{0\}$	$\{0\}$	$\{1, 0\}$	$\{0\}$	$\{1, 0\}$	$\{1, 0\}$
$\{\bot\}$	$\{\bot\}$	$\{0\}$	$\{\bot\}$	$\{\bot\}$	$\{0, \bot\}$	$\{0, \bot\}$	$\{0, \bot\}$
$\{1, \bot\}$	$\{1, \bot\}$	$\{1, 0\}$	$\{\bot\}$	$\{1, \bot\}$	$\{1, 0, \bot\}$	$\{1, 0, \bot\}$	$\{1, 0, \bot\}$
$\{0, \bot\}$	$\{1, \bot\}$	$\{0\}$	$\{0, \bot\}$	$\{1, 0, \bot\}$	$\{0, \bot\}$	$\{1, 0, \bot\}$	$\{1, 0, \bot\}$
$\{1, 0\}$	$\{1\}$	$\{1, 0\}$	$\{0, \bot\}$	$\{1, 0, \bot\}$	$\{1, 0, \bot\}$	$\{1, 0\}$	$\{1, 0, \bot\}$
$\{1, 0, \bot\}$	$\{1, \bot\}$	$\{1, 0\}$	$\{0, \bot\}$	$\{1, 0, \bot\}$	$\{1, 0, \bot\}$	$\{1, 0, \bot\}$	$\{1, 0, \bot\}$

Solution (c) Decisions $\{1, 0\}$ and $\{1, 0, \bot\}$ should have the same behavior because $\rho_{76}(\{1, 0\}) = \rho_{76}(\{1, 0, \bot\})$. However:

$\rho_{76}(\alpha(\{1, 0\}, \{1\})) = \rho_{76}(\{1\}) = P$

$\rho_{76}(\alpha(\{1, 0, \bot\}, \{1\})) = \rho_{76}(\{1, \bot\}) = I(P)$

Therefore, reduction ρ_{76} is not safe with respect to operator α.

Chapter 8

XACML

8.1 Exam 30/10/2017: Question 6

Given the XACML policy and access request below, determine the access response.

Hint: If an attribute is missing (i.e., it is not provided in the request), then MustBePresent governs the applicability of the Rule/Policy/PolicySet.

- If MustBePresent is "False" (default value), then a missing attribute results in an empty bag. (i.e., the Rule/Policy/PolicysSet is "Not Applicable")
- If MustBePresent is "True", then a missing attribute results in an error. Some combining algorithms are defined in terms of an extended set of "Indeterminate" values ("Indeterminate(P)", "Indeterminate(D)", "Indeterminate(PD)"). The extended set associated with the "Indeterminate" contains the potential effect values which could have occurred if there would not have been an error causing the "Indeterminate".

```
Access Request

  <Request>
   <Attributes
         Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject">
         <Attribute IncludeInResult="false"
            AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                Alice
            </AttributeValue>
         </Attribute>
         <Attribute IncludeInResult="false"
            AttributeId="urn:oasis:names:tc:xacml:2.0:subject:role">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                clerk
            </AttributeValue>
         </Attribute>
         <Attribute IncludeInResult="false"
            AttributeId="urn:oasis:names:tc:xacml:2.0:subject:role">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                accountant
            </AttributeValue>
         </Attribute>
    </Attributes>
    <Attributes
         Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource">
         <Attribute IncludeInResult="false"
            AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                FinacialRecord
            </AttributeValue>
         </Attribute>
    </Attributes>
    <Attributes
         Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action">
         <Attribute IncludeInResult="false"
            AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                read
            </AttributeValue>
         </Attribute>
    </Attributes>
  </Request>
```

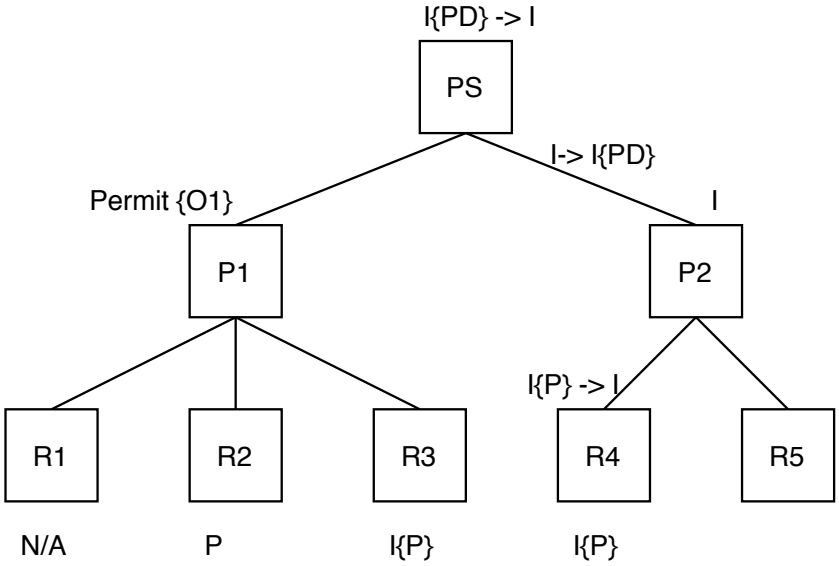
```
<PolicySet PolicySetId="PS"
  xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  PolicyCombiningAlgId="urn:oasis:names:tc:xacml:3.0:policy-combining-algorithm:deny-overrides">
  <Target>
       <AnyOf>
          <AllOf>
           <Match
             MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
             <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                 FinacialRecord
             </AttributeValue>
             <AttributeDesignator
                 MustBePresent="false"
                 Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
                 AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
                 DataType="http://www.w3.org/2001/XMLSchema#string"/>
           </Match>
          </AllOf>
        </AnyOf>
  </Target>
  <Policy PolicyId="P1"
    RuleCombiningAlgId="urn:oasis:names:tc:xacml:3.0:rule-combining-algorithm:deny-overrides">
    <Target />
    <Rule Effect="Deny" RuleId="R1">
      <Target>
       <AnyOf>
         <AllOf>
           <Match
               MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
               <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                  manager
               </AttributeValue>
               <AttributeDesignator MustBePresent="false"
                   Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                   AttributeId="urn:oasis:names:tc:xacml:2.0:example:attribute:role"
                   DataType="http://www.w3.org/2001/XMLSchema#string"/>
           </Match>
           <Match
               MatchId="urn:oasis:names:tc:xacml:1.0:function:time-greater-than">
               <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#time">
                  15:00
               </AttributeValue>
               <AttributeDesignator MustBePresent="true"
                   Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                   AttributeId="urn:oasis:names:tc:xacml:1.0:subject:authentication-time"
                   DataType="http://www.w3.org/2001/XMLSchema#time"/>
           </Match>
         </AllOf>
         <AllOf>
           <Match
               MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
```

```
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
               clerk
            </AttributeValue>
            <AttributeDesignator MustBePresent="false"
                Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                AttributeId="urn:oasis:names:tc:xacml:2.0:example:attribute:role"
                DataType="http://www.w3.org/2001/XMLSchema#string"/>
        </Match>
        <Match
            MatchId="urn:oasis:names:tc:xacml:1.0:function:time-greater-than">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#time">
               15:00
            </AttributeValue>
            <AttributeDesignator MustBePresent="false"
               Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
               AttributeId="urn:oasis:names:tc:xacml:1.0:subject:authentication-time"
               DataType="http://www.w3.org/2001/XMLSchema#time"/>
        </Match>
      </AllOf>
    </AnyOf>
  </Target>
</Rule>
<Rule Effect="Permit" RuleId="R2">
  <Target>
   <AnyOf>
     <AllOf>
       <Match
           MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
           <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
              accountant
           </AttributeValue>
           <AttributeDesignator MustBePresent="false"
               Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
               AttributeId="urn:oasis:names:tc:xacml:2.0:example:attribute:role"
               DataType="http://www.w3.org/2001/XMLSchema#string"/>
       </Match>
       <Match
           MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
           <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
              read
           </AttributeValue>
           <AttributeDesignator MustBePresent="false"
              Category="urn:oasis:names:tc:xacml:1.0:subject-category:action"
              AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
              DataType="http://www.w3.org/2001/XMLSchema#string"/>
       </Match>
     </AllOf>
    </AnyOf>
  </Target>
</Rule>
<Rule Effect="Permit" RuleId="R3">
  <Target>
```

```
      <AnyOf>
        <AllOf>
          <Match
              MatchId="urn:oasis:names:tc:xacml:1.0:function:time-greater-than">
              <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#time">
                 15:00
              </AttributeValue>
              <AttributeDesignator MustBePresent="true"
                 Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                 AttributeId="urn:oasis:names:tc:xacml:1.0:subject:authentication-time"
                 DataType="http://www.w3.org/2001/XMLSchema#time"/>
          </Match>
          <Match
              MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
              <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                 accountant
              </AttributeValue>
              <AttributeDesignator MustBePresent="false"
                  Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                  AttributeId="urn:oasis:names:tc:xacml:2.0:example:attribute:role"
                  DataType="http://www.w3.org/2001/XMLSchema#string"/>
          </Match>
        </AllOf>
       </AnyOf>
     </Target>
   </Rule>
   <Obligations>
     <Obligation FulfillOn="Permit" ObligationId="01" />
     <Obligation FulfillOn="Deny" ObligationId="02" />
   </Obligations>
</Policy>
<Policy PolicyId="P2"
   RuleCombiningAlgId="urn:oasis:names:tc:xacml:3.0:rule-combining-algorithm:first-applicable">
   <Target />
   <Rule Effect="Permit" RuleId="R4">
     <Target>
       <AnyOf>
        <AllOf>
          <Match
              MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
              <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                 clerk
              </AttributeValue>
              <AttributeDesignator MustBePresent="false"
                  Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                  AttributeId="urn:oasis:names:tc:xacml:2.0:example:attribute:role"
                  DataType="http://www.w3.org/2001/XMLSchema#string"/>
          </Match>
          <Match
              MatchId="urn:oasis:names:tc:xacml:1.0:function:time-greater-than">
              <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#time">
                 15:00
```

```
              </AttributeValue>
              <AttributeDesignator MustBePresent="true"
                  Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                  AttributeId="urn:oasis:names:tc:xacml:1.0:subject:authentication-time"
                  DataType="http://www.w3.org/2001/XMLSchema#time"/>
          </Match>
         </AllOf>
        </AnyOf>
      </Target>
    </Rule>
    <Rule Effect="Deny" RuleId="R5">
      <Target>
       <AnyOf>
         <AllOf>
           <Match
              MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
              <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                 accountant
              </AttributeValue>
              <AttributeDesignator MustBePresent="false"
                  Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                  AttributeId="urn:oasis:names:tc:xacml:2.0:example:attribute:role"
                  DataType="http://www.w3.org/2001/XMLSchema#string"/>
           </Match>
           <Match
              MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
              <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                 read
              </AttributeValue>
              <AttributeDesignator MustBePresent="false"
                 Category="urn:oasis:names:tc:xacml:1.0:subject-category:action"
                 AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
                 DataType="http://www.w3.org/2001/XMLSchema#string"/>
           </Match>
         </AllOf>
       </AnyOf>
      </Target>
    </Rule>
    <Obligations>
      <Obligation FulfillOn="Permit" ObligationId="03" />
      <Obligation FulfillOn="Deny" ObligationId="04" />
    </Obligations>
  </Policy>
  <Obligations>
    <Obligation FulfillOn="Permit" ObligationId="05" />
    <Obligation FulfillOn="Deny" ObligationId="06" />
  </Obligations>
</PolicySet>
```

Solution



8.2 Exam 22/1/2018: Question 6

Given the XACML policy and access request below, determine the access response.
Hint: If an attribute is missing (i.e., it is not provided in the request), then MustBePresent governs the applicability of the Rule/Policy/PolicySet.

- If MustBePresent is "False" (default value), then a missing attribute results in an empty bag. (i.e., the Rule/Policy/PolicysSet is "Not Applicable")
- If MustBePresent is "True", then a missing attribute results in an error. Some combining algorithms are defined in terms of an extended set of "Indeterminate" values ("Indeterminate(P)", "Indeterminate(D)", "Indeterminate(PD)"). The extended set associated with the "Indeterminate" contains the potential effect values which could have occurred if there would not have been an error causing the "Indeterminate".

```
Access Request

  <Request>
   <Attributes
         Category="urn:oasis:names:tc:xacml:3.0:subject-category:access-subject">
         <Attribute IncludeInResult="false"
            AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                Charlie
            </AttributeValue>
         </Attribute>
         <Attribute IncludeInResult="false"
            AttributeId="urn:oasis:names:tc:xacml:1.0:subject:role">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                manager
            </AttributeValue>
         </Attribute>
         <Attribute IncludeInResult="false"
            AttributeId="urn:oasis:names:tc:xacml:1.0:subject:role">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                employee
            </AttributeValue>
         </Attribute>
    </Attributes>
    <Attributes
         Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource">
         <Attribute IncludeInResult="false"
            AttributeId="urn:oasis:names:tc:xacml:1.0:resource-id">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                financialRecord
            </AttributeValue>
         </Attribute>
    </Attributes>
    <Attributes
         Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action">
         <Attribute IncludeInResult="false"
            AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                read
            </AttributeValue>
         </Attribute>
    </Attributes>
  </Request>
```

```
<PolicySet PolicySetId="PS"
   xmlns="urn:oasis:names:tc:xacml:3.0:policy:schema:os"
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   PolicyCombiningAlgId="urn:oasis:names:tc:xacml:3.0:policy-combining-algorithm:deny-overrides">
   <Target>
      <AnyOf>
        <AllOf>
          <Match
            MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                financialRecord
            </AttributeValue>
            <AttributeDesignator
                MustBePresent="false"
                Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
                AttributeId="urn:oasis:names:tc:xacml:1.0:resource-id"
                DataType="http://www.w3.org/2001/XMLSchema#string"/>
          </Match>
         </AllOf>
      </AnyOf>
   </Target>
   <Policy PolicyId="P1"
      RuleCombiningAlgId="urn:oasis:names:tc:xacml:3.0:rule-combining-algorithm:first-applicable">
      <Target>
        <AnyOf>
          <AllOf>
            <Match
              MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
              <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                  read
              </AttributeValue>
              <AttributeDesignator MustBePresent="true"
                Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
                AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
                DataType="http://www.w3.org/2001/XMLSchema#string"/>
            </Match>
          </AllOf>
        </AnyOf>
      </Target>
      <Rule Effect="Deny" RuleId="R1">
        <Target>
         <AnyOf>
           <AllOf>
             <Match
                MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                   accountant
                </AttributeValue>
                <AttributeDesignator MustBePresent="true"
                   Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                   AttributeId="urn:oasis:names:tc:xacml:1.0:subject:role"
```

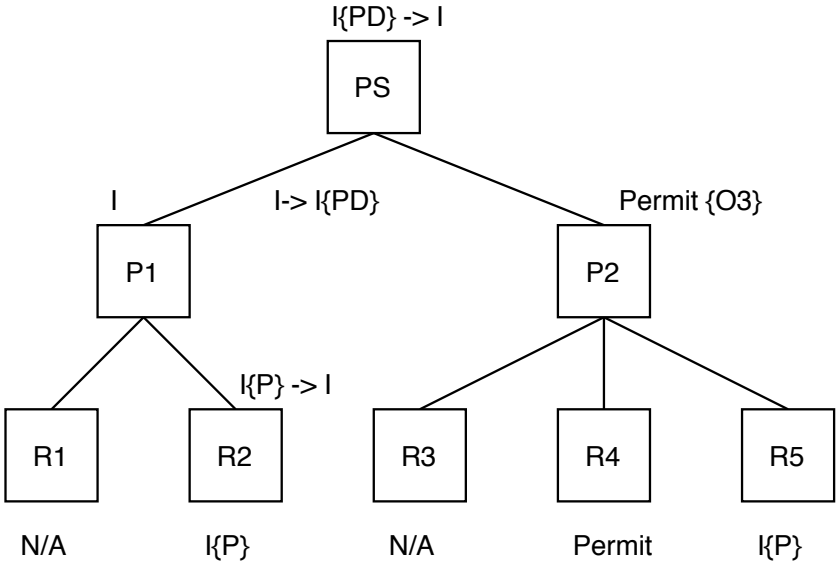
```
                DataType="http://www.w3.org/2001/XMLSchema#string"/>
          </Match>
          <Match
              MatchId="urn:oasis:names:tc:xacml:1.0:function:time-greater-than">
              <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#time">
                 14:00
              </AttributeValue>
              <AttributeDesignator MustBePresent="false"
                 Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                 AttributeId="urn:oasis:names:tc:xacml:1.0:subject:authentication-time"
                 DataType="http://www.w3.org/2001/XMLSchema#time"/>
          </Match>
         </AllOf>
       </AnyOf>
      </Target>
    </Rule>
    <Rule Effect="Permit" RuleId="R2">
      <Target>
        <AnyOf>
          <AllOf>
            <Match
              MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
              <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                 manager
              </AttributeValue>
              <AttributeDesignator MustBePresent="false"
                 Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                 AttributeId="urn:oasis:names:tc:xacml:1.0:subject:role"
                 DataType="http://www.w3.org/2001/XMLSchema#string"/>
            </Match>
            <Match
             MatchId="urn:oasis:names:tc:xacml:1.0:function:time-greater-than">
               <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#time">
                  14:00
               </AttributeValue>
               <AttributeDesignator MustBePresent="true"
                 Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                 AttributeId="urn:oasis:names:tc:xacml:1.0:subject:authentication-time"
                 DataType="http://www.w3.org/2001/XMLSchema#time"/>
            </Match>
          </AllOf>
        </AnyOf>
      </Target>
    </Rule>
    <Obligations>
      <Obligation FulfillOn="Permit" ObligationId="01" />
      <Obligation FulfillOn="Deny" ObligationId="02" />
    </Obligations>
  </Policy>
  <Policy PolicyId="P2"
    RuleCombiningAlgId="urn:oasis:names:tc:xacml:3.0:rule-combining-algorithm:permit-overrides">
    <Target />
```

```
<Rule Effect="Permit" RuleId="R3">
  <Target>
    <AnyOf>
      <AllOf>
        <Match
         MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
            employee
          </AttributeValue>
          <AttributeDesignator MustBePresent="false"
            Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
            AttributeId="urn:oasis:names:tc:xacml:1.0:subject:role"
           DataType="http://www.w3.org/2001/XMLSchema#string"/>
        </Match>
      </AllOf>
    </AnyOf>
    <AnyOf>
      <AllOf>
        <Match
         MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
          <AttributeValue  DataType="http://www.w3.org/2001/XMLSchema#string">
            accountant
          </AttributeValue>
          <AttributeDesignator MustBePresent="false"
            Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
            AttributeId="urn:oasis:names:tc:xacml:1.0:subject:role"
           DataType="http://www.w3.org/2001/XMLSchema#string"/>
        </Match>
      </AllOf>
    </AnyOf>
  </Target>
</Rule>
<Rule Effect="Permit" RuleId="R4">
  <Target>
    <AnyOf>
      <AllOf>
        <Match
          MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
              manager
          </AttributeValue>
          <AttributeDesignator MustBePresent="false"
              Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
              AttributeId="urn:oasis:names:tc:xacml:1.0:subject:role"
              DataType="http://www.w3.org/2001/XMLSchema#string"/>
        </Match>
        <Match
          MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
             write
          </AttributeValue>
          <AttributeDesignator MustBePresent="true"
```

```
                Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
                AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
                DataType="http://www.w3.org/2001/XMLSchema#string"/>
          </Match>
        </AllOf>
        <AllOf>
          <Match
            MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
               manager
            </AttributeValue>
            <AttributeDesignator MustBePresent="true"
                Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                AttributeId="urn:oasis:names:tc:xacml:1.0:subject:role"
                DataType="http://www.w3.org/2001/XMLSchema#string"/>
          </Match>
          <Match
            MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
               read
            </AttributeValue>
            <AttributeDesignator MustBePresent="true"
                Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
                AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
                DataType="http://www.w3.org/2001/XMLSchema#string"/>
          </Match>
        </AllOf>
      </AnyOf>
    </Target>
  </Rule>
  <Rule Effect="Permit" RuleId="R5">
    <Target>
      <AnyOf>
        <AllOf>
          <Match
            MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
               employee
            </AttributeValue>
            <AttributeDesignator MustBePresent="false"
                Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                AttributeId="urn:oasis:names:tc:xacml:1.0:subject:role"
                DataType="http://www.w3.org/2001/XMLSchema#string"/>
          </Match>
          <Match
            MatchId="urn:oasis:names:tc:xacml:1.0:function:time-greater-than">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#time">
               14:00
            </AttributeValue>
            <AttributeDesignator MustBePresent="true"
               Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
               AttributeId="urn:oasis:names:tc:xacml:1.0:subject:authentication-time"
```

```
                DataType="http://www.w3.org/2001/XMLSchema#time"/>
            </Match>
          </AllOf>
        </AnyOf>
      </Target>
    </Rule>
    <Obligations>
      <Obligation FulfillOn="Permit" ObligationId="03" />
      <Obligation FulfillOn="Deny" ObligationId="04" />
    </Obligations>
  </Policy>
  <Obligations>
    <Obligation FulfillOn="Permit" ObligationId="05" />
    <Obligation FulfillOn="Deny" ObligationId="06" />
  </Obligations>
</PolicySet>
```

Solution


I{PD} -> I
PS
I
I-> I{PD}
Permit {O3}
P1
P2
I{P} -> I
R1
R2
R3
R4
R5
N/A
I{P}
N/A
Permit
I{P}

8.3 Exam 2/11/2018: Question 6

Given the XACML policy and access request below, determine the access response.

Hint: If an attribute is missing (i.e., it is not provided in the request), then MustBePresent governs the applicability of the Rule/Policy/PolicySet.

- If MustBePresent is "False" (default value), then a missing attribute results in an empty bag. (i.e., the Rule/Policy/PolicysSet is "Not Applicable")
- If MustBePresent is "True", then a missing attribute results in an error. Some combining algorithms are defined in terms of an extended set of "Indeterminate" values ("Indeterminate(P)", "Indeterminate(D)", "Indeterminate(PD)"). The extended set associated with the "Indeterminate" contains the potential effect values which could have occurred if there would not have been an error causing the "Indeterminate".

```
Access Request

  <Request>
   <Attributes
         Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject">
         <Attribute IncludeInResult="false"
            AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                Bob
            </AttributeValue>
         </Attribute>
         <Attribute IncludeInResult="false"
            AttributeId="urn:oasis:names:tc:xacml:2.0:subject:role">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                manager
            </AttributeValue>
         </Attribute>
         <Attribute IncludeInResult="false"
            AttributeId="urn:oasis:names:tc:xacml:2.0:subject:role">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                accountant
            </AttributeValue>
         </Attribute>
    </Attributes>
    <Attributes
         Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource">
         <Attribute IncludeInResult="false"
            AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                FinacialRecord
            </AttributeValue>
         </Attribute>
    </Attributes>
    <Attributes
         Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action">
         <Attribute IncludeInResult="false"
            AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                write
            </AttributeValue>
         </Attribute>
    </Attributes>
  </Request>
```

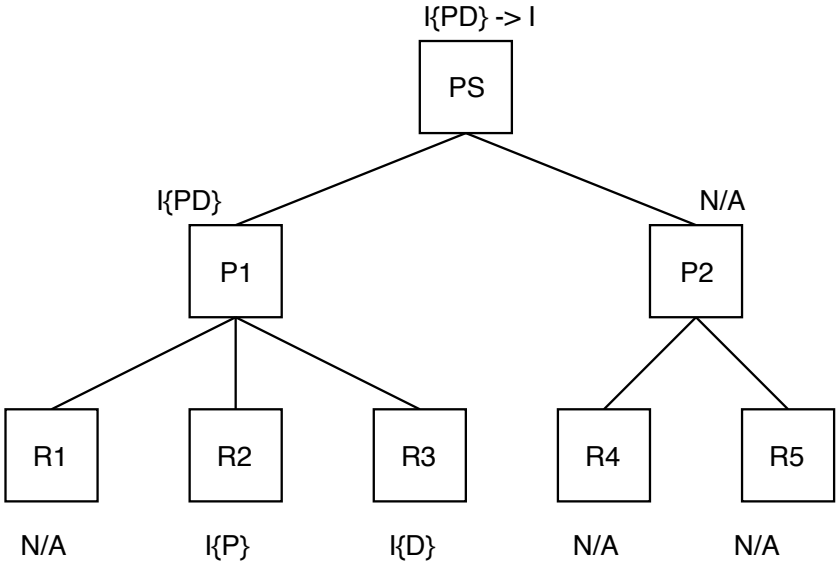
```
<PolicySet PolicySetId="PS"
  xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  PolicyCombiningAlgId="urn:oasis:names:tc:xacml:3.0:policy-combining-algorithm:deny-overrides">
  <Target>
       <AnyOf>
          <AllOf>
           <Match
             MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
             <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                 FinacialRecord
             </AttributeValue>
             <AttributeDesignator
                 MustBePresent="false"
                 Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
                 AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
                 DataType="http://www.w3.org/2001/XMLSchema#string"/>
           </Match>
          </AllOf>
        </AnyOf>
  </Target>
  <Policy PolicyId="P1"
    RuleCombiningAlgId="urn:oasis:names:tc:xacml:3.0:rule-combining-algorithm:permit-overrides">
    <Target />
    <Rule Effect="Deny" RuleId="R1">
       <Target>
        <AnyOf>
          <AllOf>
            <Match
                MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                   clerk
                </AttributeValue>
                <AttributeDesignator MustBePresent="false"
                    Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                    AttributeId="urn:oasis:names:tc:xacml:2.0:example:attribute:role"
                    DataType="http://www.w3.org/2001/XMLSchema#string"/>
            </Match>
            <Match
                MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                   write
                </AttributeValue>
                <AttributeDesignator MustBePresent="false"
                   Category="urn:oasis:names:tc:xacml:1.0:subject-category:action"
                   AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
                   DataType="http://www.w3.org/2001/XMLSchema#string"/>
            </Match>
          </AllOf>
         </AnyOf>
      </Target>
    </Rule>
```

```
<Rule Effect="Permit" RuleId="R2">
  <Target>
     <AnyOf>
       <AllOf>
         <Match
           MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
           <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
               manager
           </AttributeValue>
           <AttributeDesignator MustBePresent="false"
             Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
             AttributeId="urn:oasis:names:tc:xacml:2.0:example:attribute:role"
             DataType="http://www.w3.org/2001/XMLSchema#string"/>
         </Match>
         <Match
           MatchId="urn:oasis:names:tc:xacml:1.0:function:time-greater-than">
           <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#time">
              14:00
           </AttributeValue>
           <AttributeDesignator MustBePresent="true"
             Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
             AttributeId="urn:oasis:names:tc:xacml:1.0:subject:authentication-time"
             DataType="http://www.w3.org/2001/XMLSchema#time"/>
         </Match>
       </AllOf>
       <AllOf>
         <Match
           MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
           <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
              accountant
           </AttributeValue>
           <AttributeDesignator MustBePresent="false"
             Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
             AttributeId="urn:oasis:names:tc:xacml:2.0:example:attribute:role"
             DataType="http://www.w3.org/2001/XMLSchema#string"/>
         </Match>
         <Match
           MatchId="urn:oasis:names:tc:xacml:1.0:function:time-greater-than">
           <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#time">
              14:00
           </AttributeValue>
           <AttributeDesignator MustBePresent="false"
             Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
             AttributeId="urn:oasis:names:tc:xacml:1.0:subject:authentication-time"
             DataType="http://www.w3.org/2001/XMLSchema#time"/>
         </Match>
       </AllOf>
     </AnyOf>
  </Target>
</Rule>
<Rule Effect="Deny" RuleId="R3">
  <Target>
```

```
      <AnyOf>
        <AllOf>
          <Match
              MatchId="urn:oasis:names:tc:xacml:1.0:function:time-greater-than">
              <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#time">
                 15:00
              </AttributeValue>
              <AttributeDesignator MustBePresent="true"
                 Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                 AttributeId="urn:oasis:names:tc:xacml:1.0:subject:authentication-time"
                 DataType="http://www.w3.org/2001/XMLSchema#time"/>
          </Match>
          <Match
              MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
              <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                 manager
              </AttributeValue>
              <AttributeDesignator MustBePresent="false"
                  Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                  AttributeId="urn:oasis:names:tc:xacml:2.0:example:attribute:role"
                  DataType="http://www.w3.org/2001/XMLSchema#string"/>
          </Match>
        </AllOf>
       </AnyOf>
     </Target>
   </Rule>
   <Obligations>
     <Obligation FulfillOn="Permit" ObligationId="01" />
     <Obligation FulfillOn="Deny" ObligationId="02" />
   </Obligations>
</Policy>
<Policy PolicyId="P2"
   RuleCombiningAlgId="urn:oasis:names:tc:xacml:3.0:rule-combining-algorithm:first-applicable">
   <Target />
   <Rule Effect="Permit" RuleId="R4">
     <Target>
       <AnyOf>
        <AllOf>
          <Match
              MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
              <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                 clerk
              </AttributeValue>
              <AttributeDesignator MustBePresent="false"
                  Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                  AttributeId="urn:oasis:names:tc:xacml:2.0:example:attribute:role"
                  DataType="http://www.w3.org/2001/XMLSchema#string"/>
          </Match>
          <Match
              MatchId="urn:oasis:names:tc:xacml:1.0:function:time-greater-than">
              <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#time">
                 14:00
```

```
              </AttributeValue>
              <AttributeDesignator MustBePresent="false"
                  Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                  AttributeId="urn:oasis:names:tc:xacml:1.0:subject:authentication-time"
                  DataType="http://www.w3.org/2001/XMLSchema#time"/>
          </Match>
         </AllOf>
        </AnyOf>
      </Target>
    </Rule>
    <Rule Effect="Deny" RuleId="R5">
      <Target>
       <AnyOf>
         <AllOf>
           <Match
              MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
              <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                 manager
              </AttributeValue>
              <AttributeDesignator MustBePresent="false"
                  Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                  AttributeId="urn:oasis:names:tc:xacml:2.0:example:attribute:role"
                  DataType="http://www.w3.org/2001/XMLSchema#string"/>
           </Match>
           <Match
              MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
              <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                 read
              </AttributeValue>
              <AttributeDesignator MustBePresent="false"
                 Category="urn:oasis:names:tc:xacml:1.0:subject-category:action"
                 AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
                 DataType="http://www.w3.org/2001/XMLSchema#string"/>
           </Match>
         </AllOf>
       </AnyOf>
      </Target>
    </Rule>
    <Obligations>
      <Obligation FulfillOn="Permit" ObligationId="03" />
      <Obligation FulfillOn="Deny" ObligationId="04" />
    </Obligations>
  </Policy>
  <Obligations>
    <Obligation FulfillOn="Permit" ObligationId="05" />
    <Obligation FulfillOn="Deny" ObligationId="06" />
  </Obligations>
</PolicySet>
```

Solution



8.4 Exam 25/1/2019: Question 6

Given the XACML policy and access request below, determine the access response.
Hint: If an attribute is missing (i.e., it is not provided in the request), then MustBePresent governs the applicability of the Rule/Policy/PolicySet.

- If MustBePresent is "False" (default value), then a missing attribute results in an empty bag. (i.e., the Rule/Policy/PolicysSet is "Not Applicable")
- If MustBePresent is "True", then a missing attribute results in an error. Some combining algorithms are defined in terms of an extended set of "Indeterminate" values ("Indeterminate(P)", "Indeterminate(D)", "Indeterminate(PD)"). The extended set associated with the "Indeterminate" contains the potential effect values which could have occurred if there would not have been an error causing the "Indeterminate".

```
Access Request

  <Request>
   <Attributes
         Category="urn:oasis:names:tc:xacml:3.0:subject-category:access-subject">
         <Attribute IncludeInResult="false"
            AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                Bob
            </AttributeValue>
         </Attribute>
         <Attribute IncludeInResult="false"
            AttributeId="urn:oasis:names:tc:xacml:1.0:subject:role">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                employee
            </AttributeValue>
         </Attribute>
         <Attribute IncludeInResult="false"
            AttributeId="urn:oasis:names:tc:xacml:1.0:subject:role">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                accountant
            </AttributeValue>
         </Attribute>
    </Attributes>
    <Attributes
         Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource">
         <Attribute IncludeInResult="false"
            AttributeId="urn:oasis:names:tc:xacml:1.0:resource-id">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                financialRecord
            </AttributeValue>
         </Attribute>
    </Attributes>
    <Attributes
         Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action">
         <Attribute IncludeInResult="false"
            AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                write
            </AttributeValue>
         </Attribute>
    </Attributes>
  </Request>
```

```
<PolicySet PolicySetId="PS"
   xmlns="urn:oasis:names:tc:xacml:3.0:policy:schema:os"
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   PolicyCombiningAlgId="urn:oasis:names:tc:xacml:3.0:policy-combining-algorithm:permit-overrides">
   <Target>
      <AnyOf>
        <AllOf>
          <Match
            MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                financialRecord
            </AttributeValue>
            <AttributeDesignator
                MustBePresent="false"
                Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
                AttributeId="urn:oasis:names:tc:xacml:1.0:resource-id"
                DataType="http://www.w3.org/2001/XMLSchema#string"/>
          </Match>
         </AllOf>
      </AnyOf>
   </Target>
   <Policy PolicyId="P1"
      RuleCombiningAlgId="urn:oasis:names:tc:xacml:3.0:rule-combining-algorithm:permit-unless-deny">
      <Target />
      <Rule Effect="Deny" RuleId="R1">
        <Target>
         <AnyOf>
           <AllOf>
             <Match
                MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                   accountant
                </AttributeValue>
                <AttributeDesignator MustBePresent="false"
                   Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                   AttributeId="urn:oasis:names:tc:xacml:1.0:subject:role"
                   DataType="http://www.w3.org/2001/XMLSchema#string"/>
            </Match>
            <Match
                MatchId="urn:oasis:names:tc:xacml:1.0:function:time-greater-than">
                <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#time">
                   14:00
                </AttributeValue>
                <AttributeDesignator MustBePresent="false"
                   Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                   AttributeId="urn:oasis:names:tc:xacml:1.0:subject:authentication-time"
                   DataType="http://www.w3.org/2001/XMLSchema#time"/>
            </Match>
           </AllOf>
         </AnyOf>
        </Target>
```

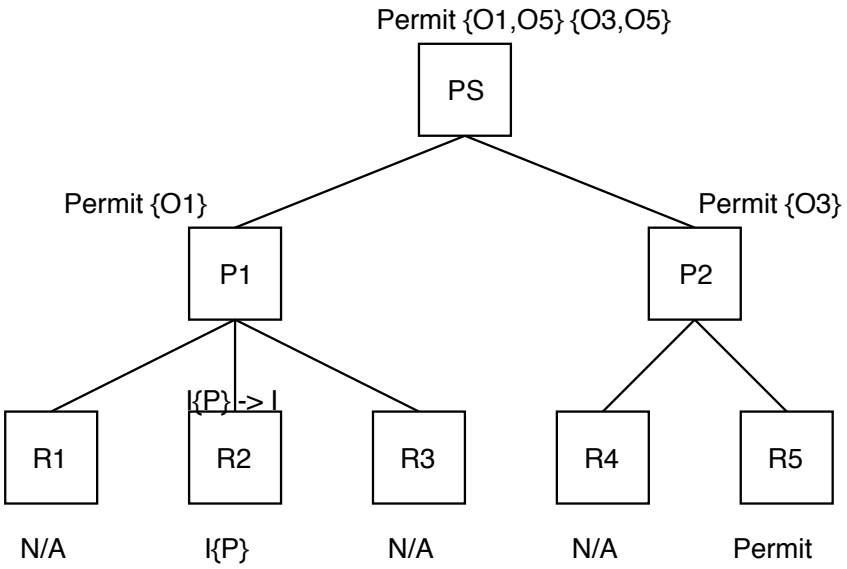
```
</Rule>
<Rule Effect="Permit" RuleId="R2">
  <Target>
    <AnyOf>
      <AllOf>
        <Match
          MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
             employee
          </AttributeValue>
          <AttributeDesignator MustBePresent="true"
             Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
             AttributeId="urn:oasis:names:tc:xacml:1.0:subject:role"
             DataType="http://www.w3.org/2001/XMLSchema#string"/>
        </Match>
        <Match
         MatchId="urn:oasis:names:tc:xacml:1.0:function:time-greater-than">
           <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#time">
              14:00
           </AttributeValue>
           <AttributeDesignator MustBePresent="true"
             Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
             AttributeId="urn:oasis:names:tc:xacml:1.0:subject:authentication-time"
             DataType="http://www.w3.org/2001/XMLSchema#time"/>
        </Match>
      </AllOf>
    </AnyOf>
  </Target>
</Rule>
<Rule Effect="Deny" RuleId="R3">
  <Target>
    <AnyOf>
      <AllOf>
        <Match
          MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
              manager
          </AttributeValue>
          <AttributeDesignator MustBePresent="false"
            Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
            AttributeId="urn:oasis:names:tc:xacml:1.0:subject:role"
            DataType="http://www.w3.org/2001/XMLSchema#string"/>
        </Match>
      </AllOf>
    </AnyOf>
    <AnyOf>
      <AllOf>
        <Match
          MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
          <AttributeValue  DataType="http://www.w3.org/2001/XMLSchema#string">
             accountant
          </AttributeValue>
```

```
            <AttributeDesignator MustBePresent="false"
              Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
              AttributeId="urn:oasis:names:tc:xacml:1.0:subject:role"
              DataType="http://www.w3.org/2001/XMLSchema#string"/>
          </Match>
        </AllOf>
      </AnyOf>
    </Target>
  </Rule>
  <Obligations>
    <Obligation FulfillOn="Permit" ObligationId="01" />
    <Obligation FulfillOn="Deny" ObligationId="02" />
  </Obligations>
</Policy>
<Policy PolicyId="P2"
  RuleCombiningAlgId="urn:oasis:names:tc:xacml:3.0:rule-combining-algorithm:first-applicable">
  <Target>
    <AnyOf>
      <AllOf>
        <Match
          MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
              write
          </AttributeValue>
          <AttributeDesignator MustBePresent="true"
            Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
            AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
            DataType="http://www.w3.org/2001/XMLSchema#string"/>
        </Match>
      </AllOf>
    </AnyOf>
  </Target>
  <Rule Effect="Permit" RuleId="R4">
  <Target>
     <AnyOf>
       <AllOf>
         <Match
           MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
           <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
               accountant
           </AttributeValue>
           <AttributeDesignator MustBePresent="false"
               Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
               AttributeId="urn:oasis:names:tc:xacml:1.0:subject:role"
               DataType="http://www.w3.org/2001/XMLSchema#string"/>
         </Match>
         <Match
           MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
           <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
              read
           </AttributeValue>
           <AttributeDesignator MustBePresent="true"
```

```
                Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
                AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
                DataType="http://www.w3.org/2001/XMLSchema#string"/>
          </Match>
        </AllOf>
        <AllOf>
          <Match
            MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
               manager
            </AttributeValue>
            <AttributeDesignator MustBePresent="true"
                Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                AttributeId="urn:oasis:names:tc:xacml:1.0:subject:role"
                DataType="http://www.w3.org/2001/XMLSchema#string"/>
          </Match>
          <Match
            MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
               write
            </AttributeValue>
            <AttributeDesignator MustBePresent="true"
                Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
                AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
                DataType="http://www.w3.org/2001/XMLSchema#string"/>
          </Match>
        </AllOf>
      </AnyOf>
    </Target>
  </Rule>
  <Rule Effect="Permit" RuleId="R5">
    <Target>
      <AnyOf>
        <AllOf>
          <Match
            MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
               employee
            </AttributeValue>
            <AttributeDesignator MustBePresent="false"
                Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                AttributeId="urn:oasis:names:tc:xacml:1.0:subject:role"
                DataType="http://www.w3.org/2001/XMLSchema#string"/>
          </Match>
          <Match
            MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
               write
            </AttributeValue>
            <AttributeDesignator MustBePresent="true"
                Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
                AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
```

```
                DataType="http://www.w3.org/2001/XMLSchema#string"/>
            </Match>
          </AllOf>
        </AnyOf>
      </Target>
    </Rule>
    <Obligations>
      <Obligation FulfillOn="Permit" ObligationId="03" />
      <Obligation FulfillOn="Deny" ObligationId="04" />
    </Obligations>
  </Policy>
  <Obligations>
    <Obligation FulfillOn="Permit" ObligationId="05" />
    <Obligation FulfillOn="Deny" ObligationId="06" />
  </Obligations>
</PolicySet>
```

Solution



8.5 Exam 1/11/2019: Question 6

Given the XACML policy and access request below, determine the access response.

Hint: If an attribute is missing (i.e., it is not provided in the request), then MustBePresent governs the applicability of the Rule/Policy/PolicySet.

- If MustBePresent is "False" (default value), then a missing attribute results in an empty bag. (i.e., the Rule/Policy/PolicysSet is "Not Applicable")
- If MustBePresent is "True", then a missing attribute results in an error. Recall that rule evaluation and some combining algorithms are defined over the extended Indeterminate set ("Indeterminate(P)", "Indeterminate(D)", "Indeterminate(PD)"). Decisions in the extended Indeterminate set indicate the potential decision(s) (Permit or Deny) that would have returned if an error have not occurred in the evaluation.

```
Access Request

<Request>
  <Attributes
    Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject">
    <Attribute IncludeInResult="false"
      AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id">
      <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
        Alice
      </AttributeValue>
    </Attribute>
    <Attribute IncludeInResult="false"
      AttributeId="urn:oasis:names:tc:xacml:2.0:subject:role">
      <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
        doctor
      </AttributeValue>
    </Attribute>
  </Attributes>
  <Attributes
    Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource">
    <Attribute IncludeInResult="false"
      AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id">
      <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
        PatientRecord
      </AttributeValue>
    </Attribute>
  </Attributes>
  <Attributes
    Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action">
    <Attribute IncludeInResult="false"
      AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id">
      <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
```

```
        write
      </AttributeValue>
    </Attribute>
  </Attributes>
</Request>
```

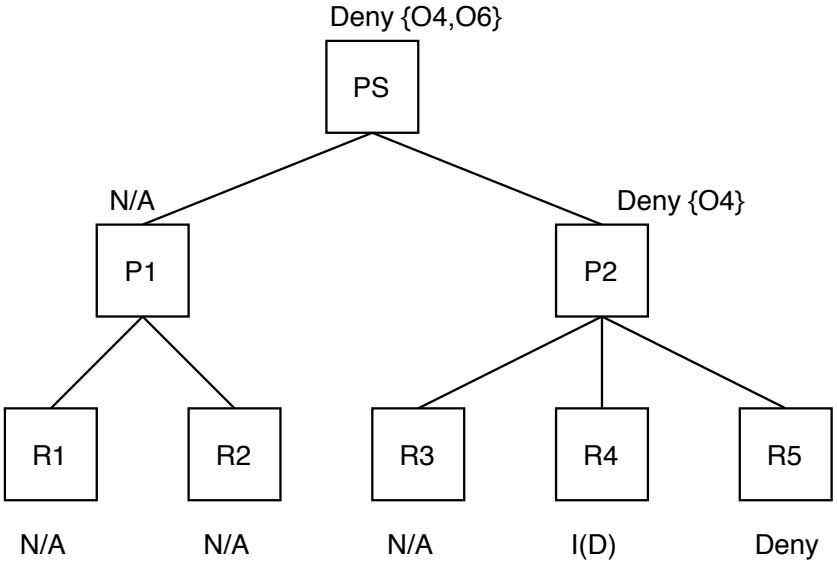
```
<PolicySet PolicySetId="PS"
  xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  PolicyCombiningAlgId="urn:oasis:names:tc:xacml:3.0:policy-combining-algorithm:deny-overrides">
  <Target>
    <AnyOf>
      <AllOf>
        <Match
          MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
            PatientRecord
          </AttributeValue>
          <AttributeDesignator
            MustBePresent="false"
            Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
            AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
            DataType="http://www.w3.org/2001/XMLSchema#string"/>
        </Match>
      </AllOf>
    </AnyOf>
  </Target>
  <Policy PolicyId="P1"
    RuleCombiningAlgId="urn:oasis:names:tc:xacml:3.0:rule-combining-algorithm:permit-overrides">
    <Target>
      <AnyOf>
        <AllOf>
          <Match
            MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
              radiology
            </AttributeValue>
            <AttributeDesignator MustBePresent="true"
              Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
              AttributeId="urn:oasis:names:tc:xacml:2.0:example:attribute:department"
              DataType="http://www.w3.org/2001/XMLSchema#string"/>
          </Match>
        </AllOf>
      </AnyOf>
    </Target>
    <Rule Effect="Deny" RuleId="R1">
      <Target>
        <AnyOf>
          <AllOf>
            <Match
              MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
              <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                doctor
              </AttributeValue>
              <AttributeDesignator MustBePresent="false"
                Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                AttributeId="urn:oasis:names:tc:xacml:2.0:example:attribute:role"
                DataType="http://www.w3.org/2001/XMLSchema#string"/>
```

```
            </Match>
            <Match
              MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
              <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                read
              </AttributeValue>
              <AttributeDesignator MustBePresent="false"
                Category="urn:oasis:names:tc:xacml:1.0:subject-category:action"
                AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
                DataType="http://www.w3.org/2001/XMLSchema#string"/>
            </Match>
          </AllOf>
        </AnyOf>
      </Target>
    </Rule>
    <Rule Effect="Permit" RuleId="R2">
      <Target>
        <AnyOf>
          <AllOf>
            <Match
              MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
              <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                nurse
              </AttributeValue>
              <AttributeDesignator MustBePresent="false"
                Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                AttributeId="urn:oasis:names:tc:xacml:2.0:example:attribute:role"
                DataType="http://www.w3.org/2001/XMLSchema#string"/>
            </Match>
            <Match
              MatchId="urn:oasis:names:tc:xacml:1.0:function:time-greater-than">
              <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#time">
                14:00
              </AttributeValue>
              <AttributeDesignator MustBePresent="true"
                Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                AttributeId="urn:oasis:names:tc:xacml:1.0:subject:authentication-time"
                DataType="http://www.w3.org/2001/XMLSchema#time"/>
            </Match>
          </AllOf>
        </AnyOf>
      </Target>
    </Rule>
    <Obligations>
      <Obligation FulfillOn="Permit" ObligationId="01" />
      <Obligation FulfillOn="Deny" ObligationId="02" />
    </Obligations>
  </Policy>
  <Policy PolicyId="P2"
    RuleCombiningAlgId="urn:oasis:names:tc:xacml:3.0:rule-combining-algorithm:permit-overrides">
    <Target />
    <Rule Effect="Permit" RuleId="R3">
```

```
    <Target>
      <AnyOf>
        <AllOf>
          <Match
            MatchId="urn:oasis:names:tc:xacml:1.0:function:time-greater-than">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#time">
              15:00
            </AttributeValue>
            <AttributeDesignator MustBePresent="false"
              Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
              AttributeId="urn:oasis:names:tc:xacml:1.0:subject:authentication-time"
              DataType="http://www.w3.org/2001/XMLSchema#time"/>
          </Match>
          <Match
            MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
              doctor
            </AttributeValue>
            <AttributeDesignator MustBePresent="false"
              Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
              AttributeId="urn:oasis:names:tc:xacml:2.0:example:attribute:role"
              DataType="http://www.w3.org/2001/XMLSchema#string"/>
          </Match>
        </AllOf>
      </AnyOf>
    </Target>
  </Rule>
  <Rule Effect="Deny" RuleId="R4">
    <Target>
      <AnyOf>
        <AllOf>
          <Match
            MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
              doctor
            </AttributeValue>
            <AttributeDesignator MustBePresent="false"
              Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
              AttributeId="urn:oasis:names:tc:xacml:2.0:example:attribute:role"
              DataType="http://www.w3.org/2001/XMLSchema#string"/>
          </Match>
          <Match
            MatchId="urn:oasis:names:tc:xacml:1.0:function:time-greater-than">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#time">
              14:00
            </AttributeValue>
            <AttributeDesignator MustBePresent="true"
              Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
              AttributeId="urn:oasis:names:tc:xacml:1.0:subject:authentication-time"
              DataType="http://www.w3.org/2001/XMLSchema#time"/>
          </Match>
        </AllOf>
```

```
        </AnyOf>
      </Target>
    </Rule>
    <Rule Effect="Deny" RuleId="R5">
      <Target>
        <AnyOf>
          <AllOf>
            <Match
              MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
              <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                doctor
              </AttributeValue>
              <AttributeDesignator MustBePresent="false"
                Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                AttributeId="urn:oasis:names:tc:xacml:2.0:example:attribute:role"
                DataType="http://www.w3.org/2001/XMLSchema#string"/>
            </Match>
            <Match
              MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
              <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                write
              </AttributeValue>
              <AttributeDesignator MustBePresent="false"
                Category="urn:oasis:names:tc:xacml:1.0:subject-category:action"
                AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
                DataType="http://www.w3.org/2001/XMLSchema#string"/>
            </Match>
          </AllOf>
        </AnyOf>
      </Target>
    </Rule>
    <Obligations>
      <Obligation FulfillOn="Permit" ObligationId="03" />
      <Obligation FulfillOn="Deny" ObligationId="04" />
    </Obligations>
  </Policy>
  <Obligations>
    <Obligation FulfillOn="Permit" ObligationId="05" />
    <Obligation FulfillOn="Deny" ObligationId="06" />
  </Obligations>
</PolicySet>
```

Solution



8.6 Exam 24/1/2020: Question 6

Given the XACML policy and access request below, determine the access response.

Hint: If an attribute is missing (i.e., it is not provided in the request), then MustBePresent governs the applicability of the Rule/Policy/PolicySet.

- If MustBePresent is "False" (default value), then a missing attribute results in an empty bag. (i.e., the Rule/Policy/PolicysSet is "Not Applicable")
- If MustBePresent is "True", then a missing attribute results in an error. Recall that rule evaluation and some combining algorithms are defined over the extended Indeterminate set ("Indeterminate(P)", "Indeterminate(D)", "Indeterminate(PD)"). Decisions in the extended Indeterminate set indicate the potential decision(s) (Permit or Deny) that would have returned if an error have not occurred in the evaluation.

```
Access Request

<Request>
  <Attributes
    Category="urn:oasis:names:tc:xacml:3.0:attribute-category:subject">
    <Attribute IncludeInResult="false"
      AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id">
      <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
        Charlie
      </AttributeValue>
    </Attribute>
    <Attribute IncludeInResult="false"
      AttributeId="urn:oasis:names:tc:xacml:2.0:subject:role">
      <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
        clerk
      </AttributeValue>
    </Attribute>
    <Attribute IncludeInResult="false"
      AttributeId="urn:oasis:names:tc:xacml:2.0:subject:role">
      <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
        accountant
      </AttributeValue>
    </Attribute>
  </Attributes>
  <Attributes
    Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource">
    <Attribute IncludeInResult="false"
      AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id">
      <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
        finacialRecord
      </AttributeValue>
    </Attribute>
```

```
  </Attributes>
  <Attributes
    Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action">
    <Attribute IncludeInResult="false"
      AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id">
      <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
        write
      </AttributeValue>
    </Attribute>
  </Attributes>
</Request>
```

```
<PolicySet PolicySetId="PS"
  xmlns="urn:oasis:names:tc:xacml:3.0:policy:schema:os"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  PolicyCombiningAlgId="urn:oasis:names:tc:xacml:3.0:policy-combining-algorithm:permit-overrides">
  <Target>
    <AnyOf>
      <AllOf>
        <Match
          MatchId="urn:oasis:names:tc:xacml:1.0:function:function:string">
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
            finacialRecord
          </AttributeValue>
          <AttributeDesignator
            MustBePresent="false"
            Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
            AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
            DataType="http://www.w3.org/2001/XMLSchema#string"/>
        </Match>
      </AllOf>
    </AnyOf>
  </Target>
  <Policy PolicyId="P1"
    RuleCombiningAlgId="urn:oasis:names:tc:xacml:2.0:rule-combining-algorithm:first-applicable">
    <Target>
      <AnyOf>
        <AllOf>
          <Match
            MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
              clerk
            </AttributeValue>
            <AttributeDesignator
              MustBePresent="true"
              Category="urn:oasis:names:tc:xacml:3.0:attribute-category:subject"
              AttributeId="urn:oasis:names:tc:xacml:2.0:example:attribute:role"
              DataType="http://www.w3.org/2001/XMLSchema#string"/>
          </Match>
        </AllOf>
      </AnyOf>
    </Target>
    <Rule Effect="Permit" RuleId="R1">
      <Target>
        <AnyOf>
          <AllOf>
            <Match
              MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
              <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                accountant
              </AttributeValue>
              <AttributeDesignator
                MustBePresent="false"
                Category="urn:oasis:names:tc:xacml:3.0:attribute-category:subject"
```

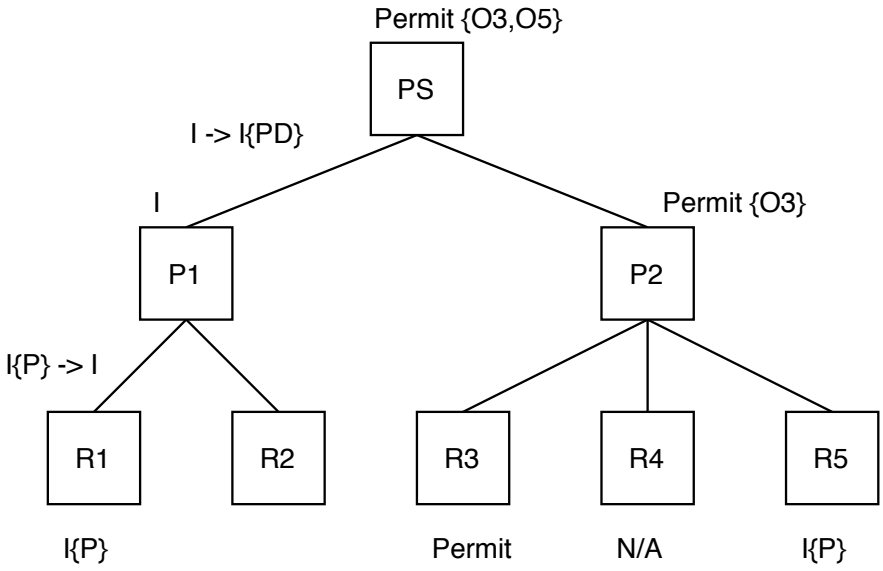
```
            AttributeId="urn:oasis:names:tc:xacml:2.0:example:attribute:role"
            DataType="http://www.w3.org/2001/XMLSchema#string"/>
        </Match>
        <Match
          MatchId="urn:oasis:names:tc:xacml:1.0:function:time-greater-than">
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#time">
            9:00
          </AttributeValue>
          <AttributeDesignator
            MustBePresent="true"
            Category="urn:oasis:names:tc:xacml:3.0:subject-category:access-subject"
            AttributeId="urn:oasis:names:tc:xacml:1.0:subject:authentication-time"
            DataType="http://www.w3.org/2001/XMLSchema#time"/>
        </Match>
      </AllOf>
    </AnyOf>
  </Target>
</Rule>
<Rule Effect="Deny" RuleId="R2">
  <Target>
    <AnyOf>
      <AllOf>
        <Match
          MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
            clerk
          </AttributeValue>
          <AttributeDesignator
            MustBePresent="false"
            Category="urn:oasis:names:tc:xacml:3.0:attribute-category:subject"
            AttributeId="urn:oasis:names:tc:xacml:2.0:example:attribute:role"
            DataType="http://www.w3.org/2001/XMLSchema#string"/>
        </Match>
        <Match
          MatchId="urn:oasis:names:tc:xacml:1.0:function:time-greater-than">
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#time">
            9:00
          </AttributeValue>
          <AttributeDesignator
            MustBePresent="false"
            Category="urn:oasis:names:tc:xacml:3.0:subject-category:access-subject"
            AttributeId="urn:oasis:names:tc:xacml:1.0:subject:authentication-time"
            DataType="http://www.w3.org/2001/XMLSchema#time"/>
        </Match>
      </AllOf>
    </AnyOf>
  </Target>
</Rule>
<Obligations>
  <Obligation FulfillOn="Permit" ObligationId="01" />
  <Obligation FulfillOn="Deny" ObligationId="02" />
</Obligations>
```

```
</Policy>
<Policy PolicyId="P2"
  RuleCombiningAlgId="urn:oasis:names:tc:xacml:3.0:rule-combining-algorithm:deny-overrides">
  <Target>
    <AnyOf>
      <AllOf>
        <Match
          MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
            write
          </AttributeValue>
          <AttributeDesignator
            MustBePresent="true"
            Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
            AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
            DataType="http://www.w3.org/2001/XMLSchema#string"/>
        </Match>
      </AllOf>
    </AnyOf>
  </Target>
  <Rule Effect="Permit" RuleId="R3">
    <Target>
      <AnyOf>
        <AllOf>
          <Match
            MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
              manager
            </AttributeValue>
            <AttributeDesignator
              MustBePresent="false"
              Category="urn:oasis:names:tc:xacml:3.0:attribute-category:subject"
              AttributeId="urn:oasis:names:tc:xacml:2.0:example:attribute:role"
              DataType="http://www.w3.org/2001/XMLSchema#string"/>
          </Match>
        </AllOf>
        <AllOf>
          <Match
            MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
              accountant
            </AttributeValue>
            <AttributeDesignator
              MustBePresent="false"
              Category="urn:oasis:names:tc:xacml:3.0:attribute-category:subject"
              AttributeId="urn:oasis:names:tc:xacml:2.0:example:attribute:role"
              DataType="http://www.w3.org/2001/XMLSchema#string"/>
          </Match>
        </AllOf>
      </AnyOf>
    </Target>
  </Rule>
```

```
<Rule Effect="Deny" RuleId="R4">
  <Target>
    <AnyOf>
      <AllOf>
        <Match
          MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
            manager
          </AttributeValue>
          <AttributeDesignator
            MustBePresent="false"
            Category="urn:oasis:names:tc:xacml:3.0:attribute-category:subject"
            AttributeId="urn:oasis:names:tc:xacml:2.0:example:attribute:role"
            DataType="http://www.w3.org/2001/XMLSchema#string"/>
        </Match>
        <Match
          MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
            accountant
          </AttributeValue>
          <AttributeDesignator
            MustBePresent="false"
            Category="urn:oasis:names:tc:xacml:3.0:attribute-category:subject"
            AttributeId="urn:oasis:names:tc:xacml:2.0:example:attribute:role"
            DataType="http://www.w3.org/2001/XMLSchema#string"/>
        </Match>
      </AllOf>
    </AnyOf>
  </Target>
</Rule>
<Rule Effect="Permit" RuleId="R5">
  <Target>
   <AnyOf>
     <AllOf>
       <Match
         MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
         <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
           clerk
         </AttributeValue>
         <AttributeDesignator
           MustBePresent="false"
           Category="urn:oasis:names:tc:xacml:3.0:attribute-category:subject"
           AttributeId="urn:oasis:names:tc:xacml:2.0:example:attribute:role"
           DataType="http://www.w3.org/2001/XMLSchema#string"/>
       </Match>
       <Match
         MatchId="urn:oasis:names:tc:xacml:1.0:function:time-greater-than">
         <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#time">
           9:00
         </AttributeValue>
         <AttributeDesignator
           MustBePresent="true"
```

```
                Category="urn:oasis:names:tc:xacml:3.0:subject-category:access-subject"
                AttributeId="urn:oasis:names:tc:xacml:1.0:subject:authentication-time"
                DataType="http://www.w3.org/2001/XMLSchema#time"/>
            </Match>
          </AllOf>
        </AnyOf>
      </Target>
    </Rule>
    <Obligations>
      <Obligation FulfillOn="Permit" ObligationId="03" />
      <Obligation FulfillOn="Deny" ObligationId="04" />
    </Obligations>
  </Policy>
  <Obligations>
    <Obligation FulfillOn="Permit" ObligationId="05" />
    <Obligation FulfillOn="Deny" ObligationId="06" />
  </Obligations>
</PolicySet>
```

Solution



8.7 Exam 18/1/2021: Part B Question 3

Given the XACML policy and access request below, determine the access response.

Hint: If an attribute is missing (i.e., it is not provided in the request), then MustBePresent governs the applicability of the Rule/Policy/PolicySet.

- If MustBePresent is "False" (default value), then a missing attribute results in an empty bag. (i.e., the Rule/Policy/PolicysSet is "Not Applicable")
- If MustBePresent is "True", then a missing attribute results in an error. Recall that rule evaluation and some combining algorithms are defined over the extended Indeterminate set ("Indeterminate(P)", "Indeterminate(D)", "Indeterminate(PD)"). Decisions in the extended Indeterminate set indicate the potential decision(s) (Permit or Deny) that would have returned if an error have not occurred in the evaluation.

```
Access Request

  <Request>
    <Attributes
         Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject">
         <Attribute IncludeInResult="false"
            AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                Bob
            </AttributeValue>
         </Attribute>
         <Attribute IncludeInResult="false"
            AttributeId="urn:oasis:names:tc:xacml:2.0:subject:role">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                nurse
            </AttributeValue>
         </Attribute>
    </Attributes>
    <Attributes
         Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource">
         <Attribute IncludeInResult="false"
            AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                PatientRecord
            </AttributeValue>
         </Attribute>
    </Attributes>
    <Attributes
         Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action">
         <Attribute IncludeInResult="false"
            AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
```

```
                read
            </AttributeValue>
        </Attribute>
    </Attributes>
</Request>
```

```
<PolicySet PolicySetId="PS"
  xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  PolicyCombiningAlgId="urn:oasis:names:tc:xacml:3.0:policy-combining-algorithm:deny-overrides">
  <Target>
    <AnyOf>
      <AllOf>
        <Match
           MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
           <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
               read
           </AttributeValue>
           <AttributeDesignator
               MustBePresent="false"
               Category="urn:oasis:names:tc:xacml:1.0:subject-category:action"
               AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
               DataType="http://www.w3.org/2001/XMLSchema#string"/>
        </Match>
      </AllOf>
    </AnyOf>
  </Target>
  <Policy PolicyId="P1"
    RuleCombiningAlgId="urn:oasis:names:tc:xacml:3.0:rule-combining-algorithm:permit-unless-deny">
    <Target />
    <Rule Effect="Permit" RuleId="R1">
      <Target>
        <AnyOf>
          <AllOf>
            <Match
               MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
               <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                   nurse
               </AttributeValue>
               <AttributeDesignator MustBePresent="false"
                   Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                   AttributeId="urn:oasis:names:tc:xacml:2.0:example:attribute:role"
                   DataType="http://www.w3.org/2001/XMLSchema#string"/>
            </Match>
            <Match
               MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
               <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                   write
               </AttributeValue>
               <AttributeDesignator MustBePresent="false"
                   Category="urn:oasis:names:tc:xacml:1.0:subject-category:action"
                   AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
                   DataType="http://www.w3.org/2001/XMLSchema#string"/>
            </Match>
          </AllOf>
        </AnyOf>
      </Target>
    </Rule>
```

```
<Rule Effect="Deny" RuleId="R2">
  <Target>
    <AnyOf>
      <AllOf>
        <Match
           MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
           <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
               nurse
           </AttributeValue>
           <AttributeDesignator MustBePresent="false"
               Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
               AttributeId="urn:oasis:names:tc:xacml:2.0:example:attribute:role"
               DataType="http://www.w3.org/2001/XMLSchema#string"/>
        </Match>
        <Match
           MatchId="urn:oasis:names:tc:xacml:1.0:function:time-greater-than">
           <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#time">
               14:00
           </AttributeValue>
           <AttributeDesignator MustBePresent="true"
               Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
               AttributeId="urn:oasis:names:tc:xacml:1.0:subject:authentication-time"
               DataType="http://www.w3.org/2001/XMLSchema#time"/>
        </Match>
      </AllOf>
    </AnyOf>
  </Target>
</Rule>
<Rule Effect="Deny" RuleId="R3">
  <Target>
    <AnyOf>
      <AllOf>
        <Match
          MatchId="urn:oasis:names:tc:xacml:1.0:function:time-greater-than">
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#time">
             15:00
          </AttributeValue>
          <AttributeDesignator MustBePresent="false"
            Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
            AttributeId="urn:oasis:names:tc:xacml:1.0:subject:authentication-time"
            DataType="http://www.w3.org/2001/XMLSchema#time"/>
        </Match>
      </AllOf>
    </AnyOf>
    <AnyOf>
      <AllOf>
        <Match
          MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
            nurse
          </AttributeValue>
          <AttributeDesignator MustBePresent="false"
```

```
                Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                AttributeId="urn:oasis:names:tc:xacml:2.0:example:attribute:role"
                DataType="http://www.w3.org/2001/XMLSchema#string"/>
            </Match>
          </AllOf>
        </AnyOf>
      </Target>
    </Rule>
    <Obligations>
      <Obligation FulfillOn="Permit" ObligationId="01" />
      <Obligation FulfillOn="Deny" ObligationId="02" />
    </Obligations>
  </Policy>
  <Policy PolicyId="P2"
    RuleCombiningAlgId="urn:oasis:names:tc:xacml:3.0:rule-combining-algorithm:permit-overrides">
    <Target />
    <Rule Effect="Deny" RuleId="R4">
      <Target>
        <AnyOf>
          <AllOf>
            <Match
               MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
               <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                   nurse
               </AttributeValue>
               <AttributeDesignator MustBePresent="false"
                   Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                   AttributeId="urn:oasis:names:tc:xacml:2.0:example:attribute:role"
                   DataType="http://www.w3.org/2001/XMLSchema#string"/>
            </Match>
            <Match
               MatchId="urn:oasis:names:tc:xacml:1.0:function:time-greater-than">
               <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#time">
                   14:00
               </AttributeValue>
               <AttributeDesignator MustBePresent="false"
                   Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                   AttributeId="urn:oasis:names:tc:xacml:1.0:subject:authentication-time"
                   DataType="http://www.w3.org/2001/XMLSchema#time"/>
            </Match>
          </AllOf>
        </AnyOf>
      </Target>
    </Rule>
    <Rule Effect="Permit" RuleId="R5">
      <Target>
        <AnyOf>
          <AllOf>
            <Match
               MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
               <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                  nurse
```

```
            </AttributeValue>
            <AttributeDesignator MustBePresent="false"
               Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
               AttributeId="urn:oasis:names:tc:xacml:2.0:example:attribute:role"
               DataType="http://www.w3.org/2001/XMLSchema#string"/>
         </Match>
         <Match
            MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
               write
            </AttributeValue>
            <AttributeDesignator MustBePresent="true"
               Category="urn:oasis:names:tc:xacml:1.0:subject-category:action"
               AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
               DataType="http://www.w3.org/2001/XMLSchema#string"/>
         </Match>
       </AllOf>
     </AnyOf>
   </Target>
  </Rule>
  <Obligations>
    <Obligation FulfillOn="Permit" ObligationId="03" />
    <Obligation FulfillOn="Deny" ObligationId="04" />
  </Obligations>
 </Policy>
 <Obligations>
   <Obligation FulfillOn="Permit" ObligationId="05" />
   <Obligation FulfillOn="Deny" ObligationId="06" />
 </Obligations>
</PolicySet>
```

Solution