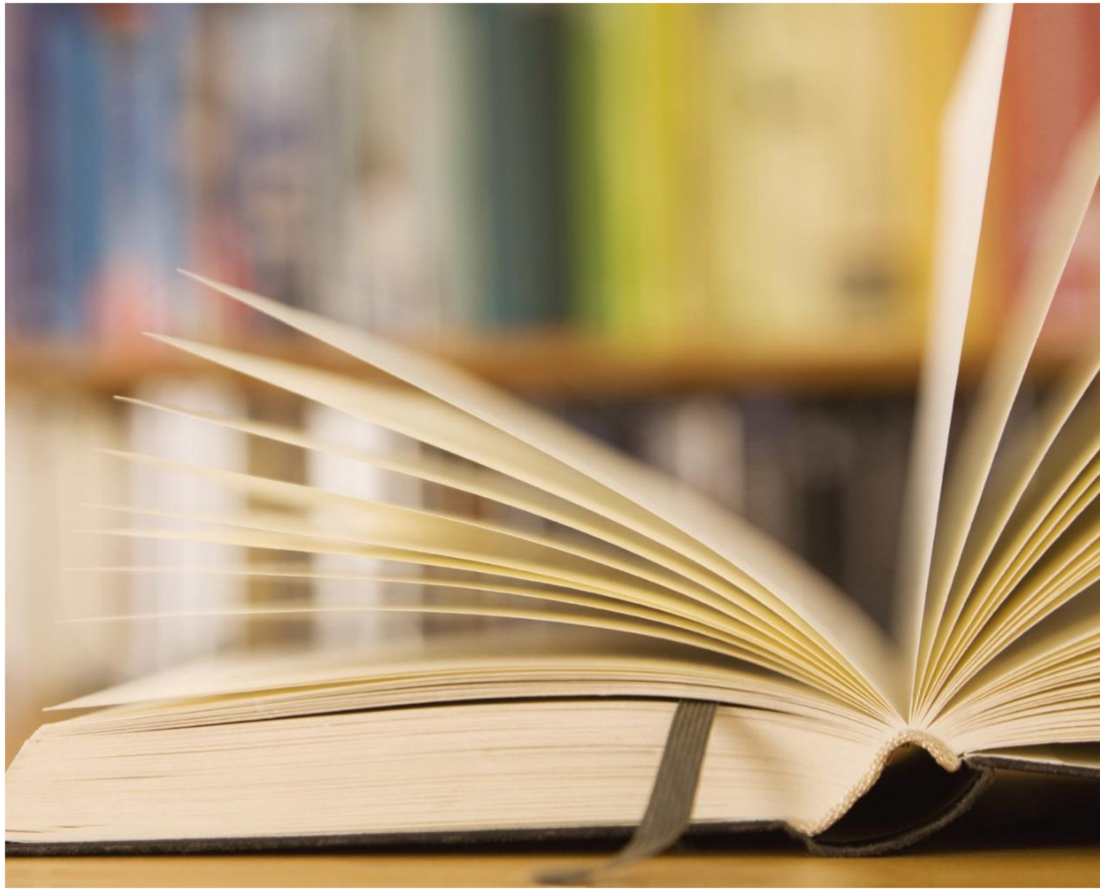
BLP Lattice Structure

Example

sjapit@uow.edu.au

10 October 2022



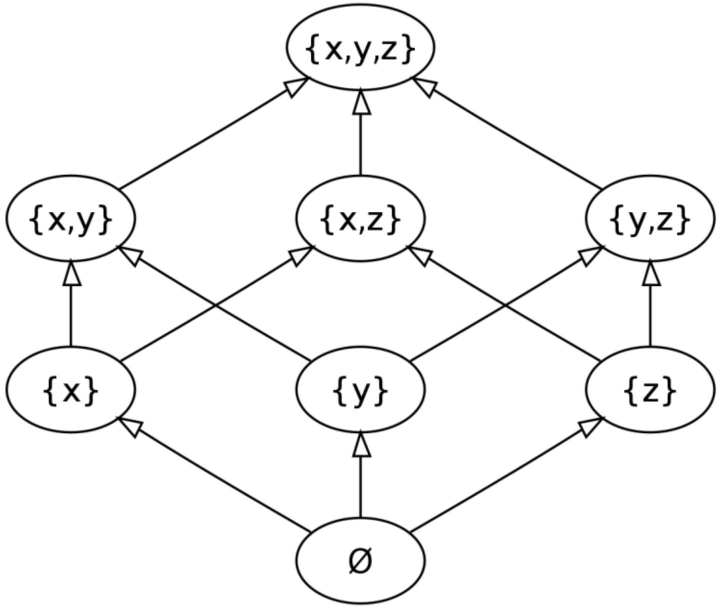
Given the following access control matrix:

	O1	O2	O3	O4	O5
S1	R	R	RW	R	R
S2	R	R	W	W	W
S3	R	R			
S4	R	R	W	R	
S5	R	R	W		W

Generate a BLP lattice-structured system where the objects and subjects are appropriately levelled to give access consistent with the access control matrix shown.

What is a lattice?

- A lattice is a partially ordered set (POSET) in which every pair of elements has both a least upper bound and a greatest lower bound.



https://en.wikipedia.org/wiki/Partially_ordered_set

What is a partially order relation?

$$R = \{(a,b) \in A \times A \mid \ a \mid b\} \quad A \in \mathbb{Z}$$

Reflexive: *if for all* $a \in A$, $(a,a) \in R$	$a \mid a$ *and* $a \in A$
Antisymmetric: *if* $(a,b) \in R$ *and* $(b,a) \in R$ *then* $a = b$	$a \mid b$ *then* $b \mid a$ *only if* $a = b$
Transitive: *if* $(a,b) \in R$ *and* $(b,c) \in R$ *then* $(a,c) \in R$	$a \mid b$ *and* $b \mid c$ *then* $a \mid c$

BLP properties (Rules)

- Ss-property
  - Subject S(n) can WRITE object O(n) iff level of clearance of subject L(S) is less than or equal the level of clearance of the object L(O), that is, $L(S) \leq L(O)$, and the subject has permission to WRITE the object.

- *-property
  - Subject S(n) can READ object O(n) iff level of clearance of subject L(S) is greater than or equal (dominant) the level of object L(O), that is, $L(S) \geq L(O)$, and the subject has permission to READ the object.

- Discretionary
  - Subject S(n) can discretionarily transfer his/her authorization to Subject at a different clearance level (subject to organization policy).

Given the following access control matrix:

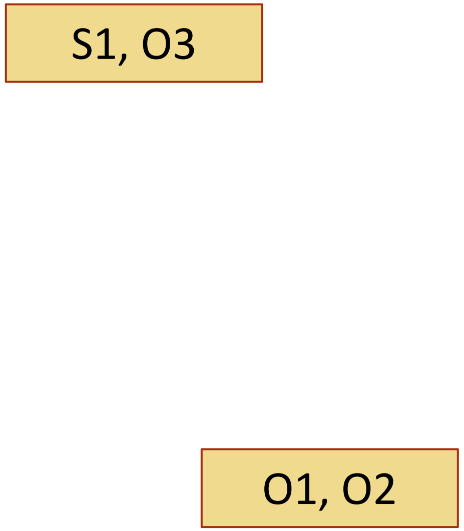
	O1	O2	O3	O4	O5
S1	R	R	RW	R	R
S2	R	R	W	W	W
S3	R	R			
S4	R	R	W	R	
S5	R	R	W		W

O1, O2 ← greatest lower bound

Subjects from every level can read objects O1 and O2 -> O1 and O2 are dominated by all subject. Hence O1 and O2 must be at the lowest point.

Given the following access control matrix:

	O1	O2	O3	O4	O5
S1	R	R	RW	R	R
S2	R	R	W	W	W
S3	R	R			
S4	R	R	W	R	
S5	R	R	W		W



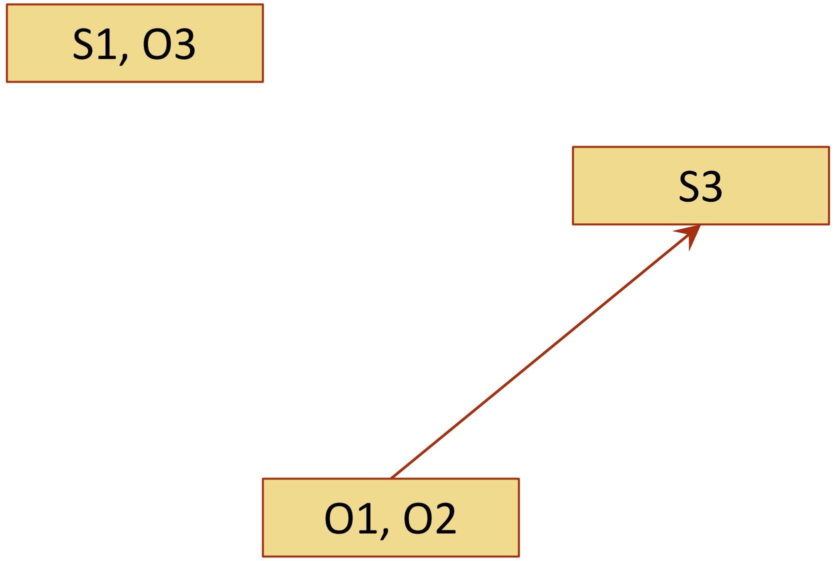
S1, O3

O1, O2

Subject S1 can read and write object O3, hence S1 and O3 must be at the same level (can put them together.)

Given the following access control matrix:

	O1	O2	O3	O4	O5
S1	R	R	RW	R	R
S2	R	R	W	W	W
S3	R	R			
S4	R	R	W	R	
S5	R	R	W		W


S1, O3

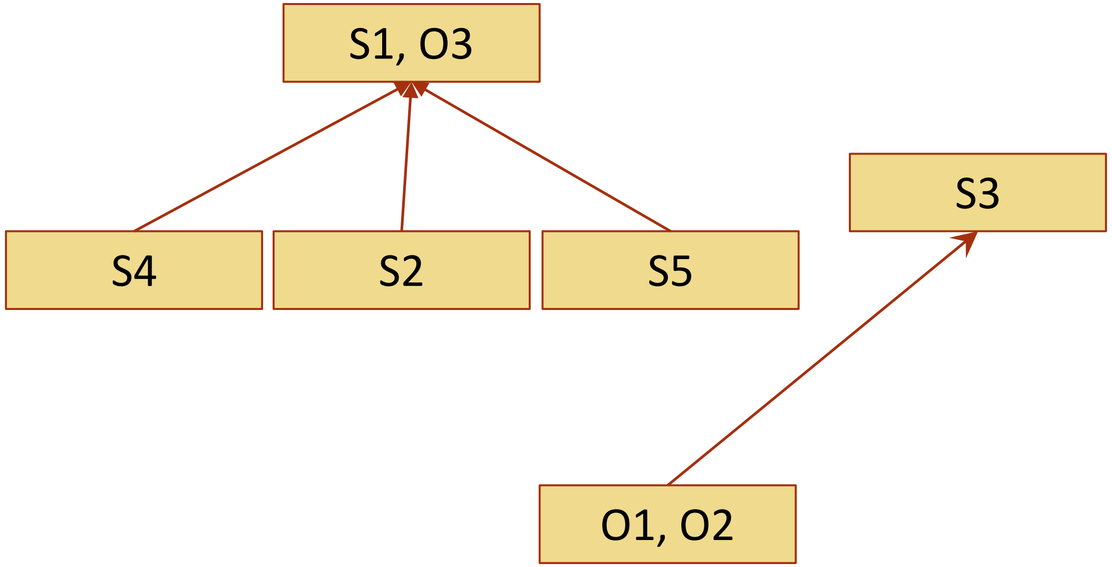
S3

O1, O2

Subject S3 can read only objects O1 and O2, hence subject S3 can only dominate object O1 and O2.

Given the following access control matrix:

	O1	O2	O3	O4	O5
S1	R	R	RW	R	R
S2	R	R	W	W	W
S3	R	R			
S4	R	R	W	R	
S5	R	R	W		W



S1, O3

S4

S2

S5

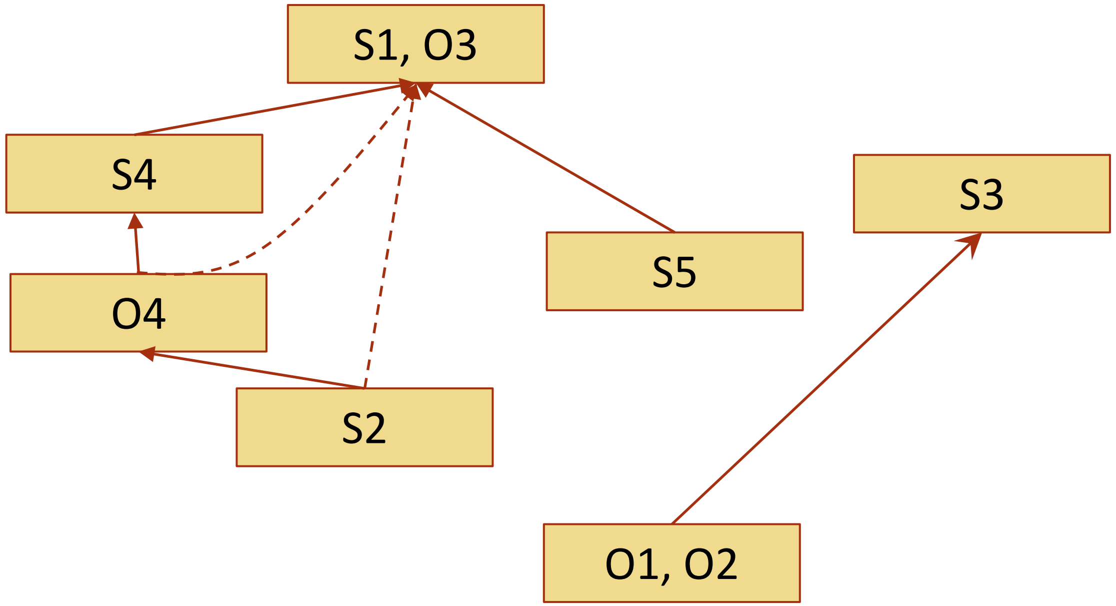
S3

O1, O2

S1 and O3 must dominate subjects S2, S4 and S5 in order to allow writing.

Given the following access control matrix:

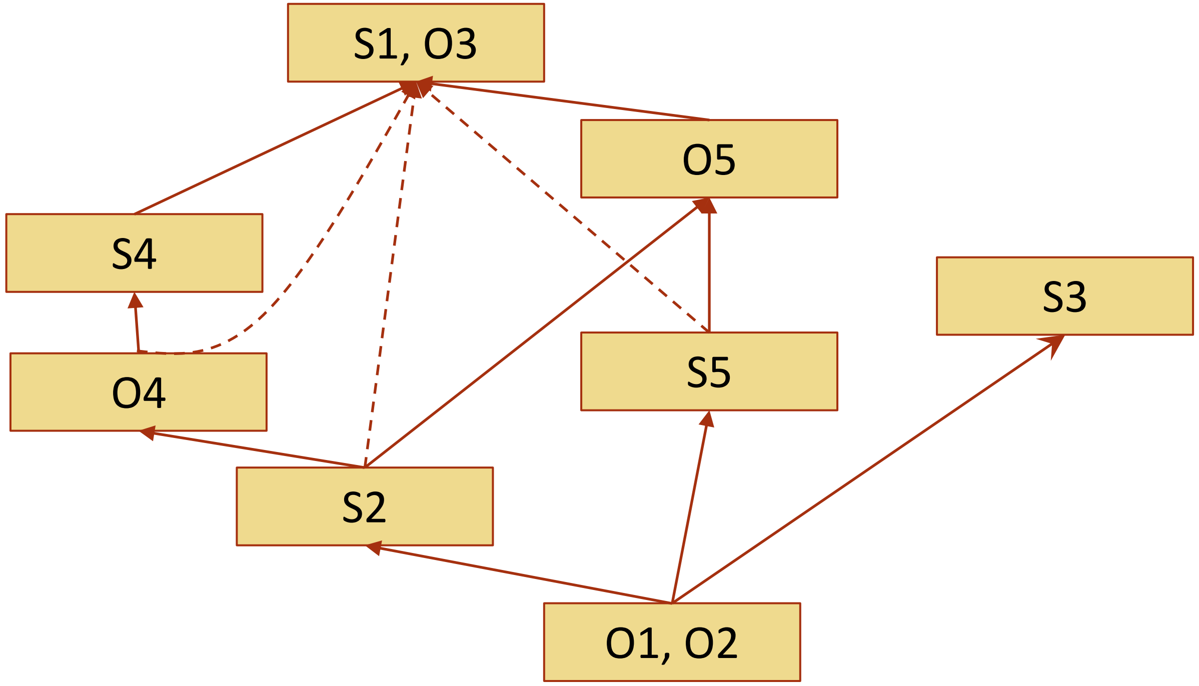
	O1	O2	O3	O4	O5
S1	R	R	RW	R	R
S2	R	R	W	W	W
S3	R	R			
S4	R	R	W	R	
S5	R	R	W		W



Subjects S2 and S4 are not at the same level due to the different behaviour with respect to O4.

Given the following access control matrix:

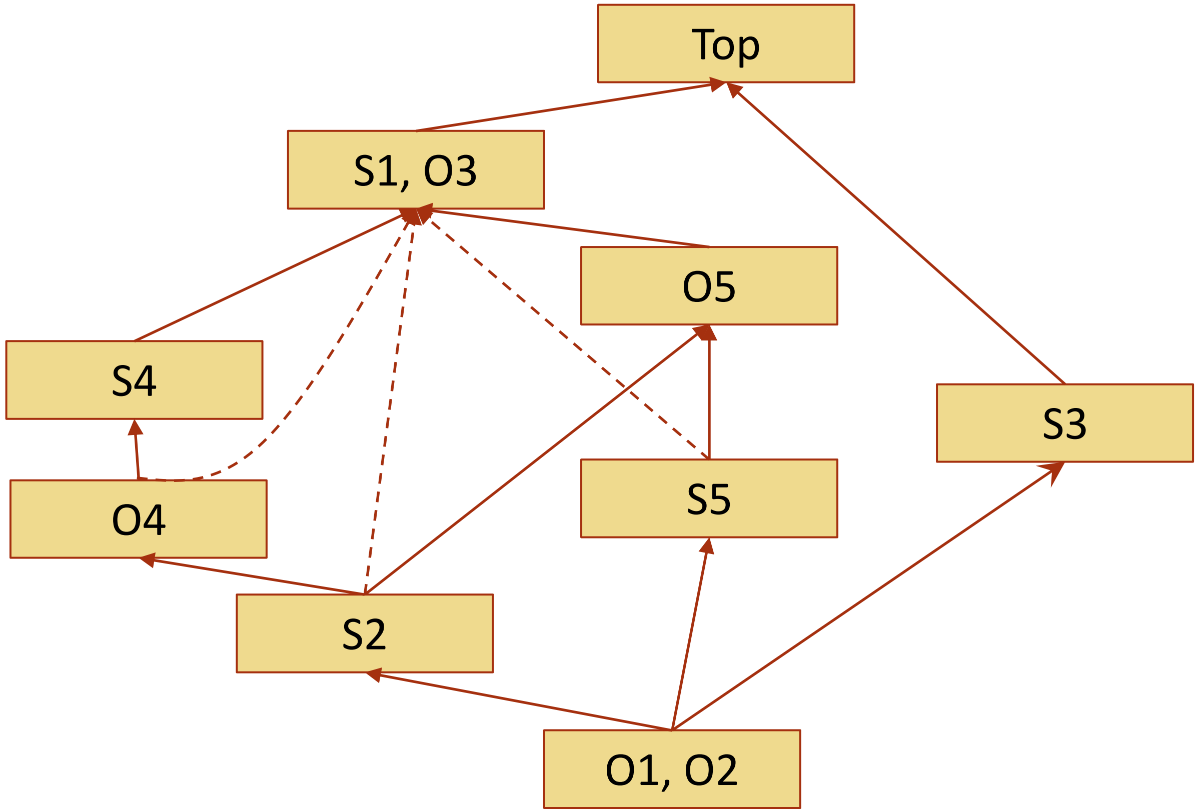
	O1	O2	O3	O4	O5
S1	R	R	RW	R	R
S2	R	R	W	W	W
S3	R	R			
S4	R	R	W	R	
S5	R	R	W		W



Complete the other dominance.

Given the following access control matrix:

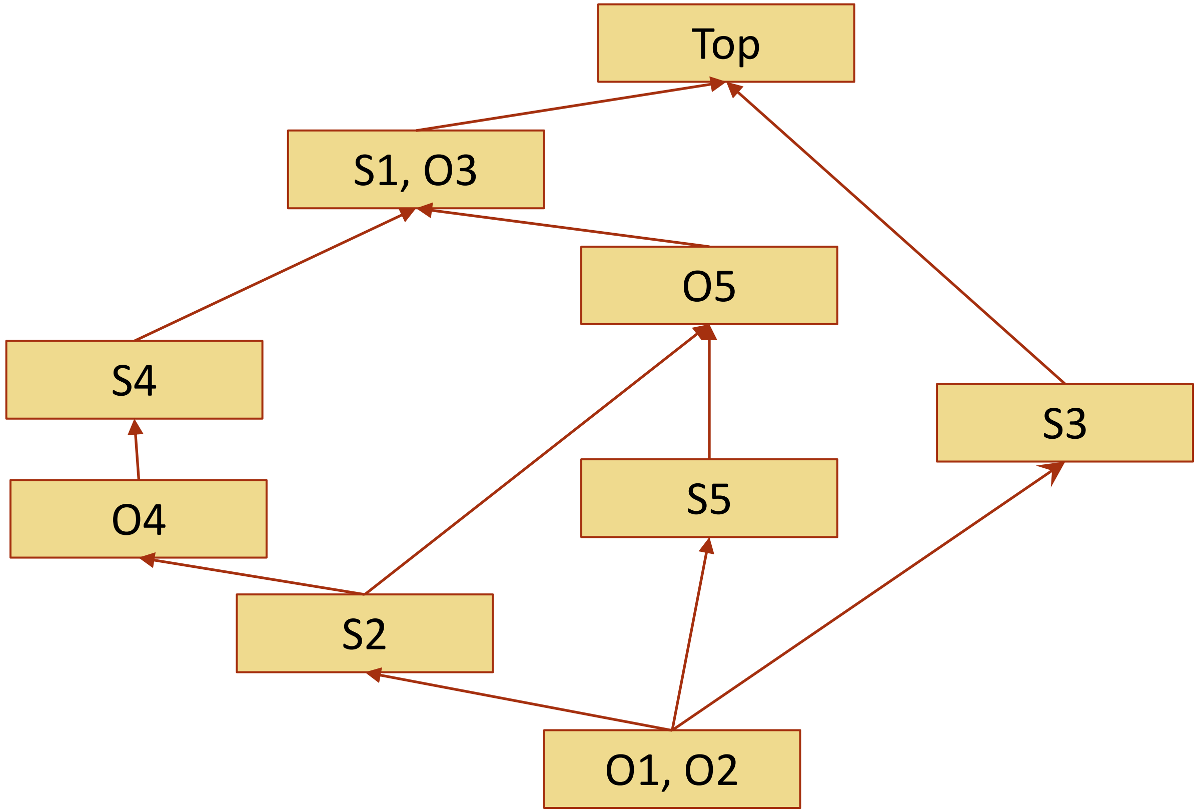
	O1	O2	O3	O4	O5
S1	R	R	RW	R	R
S2	R	R	W	W	W
S3	R	R			
S4	R	R	W	R	
S5	R	R	W		W



Introduce a top level to complete the lattice.

Given the following access control matrix:

	O1	O2	O3	O4	O5
S1	R	R	RW	R	R
S2	R	R	W	W	W
S3	R	R			
S4	R	R	W	R	
S5	R	R	W		W



Final complete lattice.