

(35 points) Access Control

10 points) You are planning to use BLP for access control in your organization. There are 4 hierarchical components Top-Secret (TS) > Secret (S) > Confidential (C) > Public (P) and 5 domains (A, B, C, D, E). Your organization has 3 users John, Pete, and Mary) and 4 files (File1, File2, File3, and File4). The security labels of the users and files are given below.

$\lambda(\text{John}) = (\text{TS}, \{A, B, C, D, E\})$
 $\lambda(\text{Pete}) = (\text{S}, \{B, C\})$
 $\lambda(\text{Mary}) = (\text{P}, \{\})$

$\lambda(\text{File1}) = (\text{S}, \{C\})$
 $\lambda(\text{File2}) = (\text{TS}, \{A, B\})$
 $\lambda(\text{File3}) = (\text{P}, \{\})$
 $\lambda(\text{File4}) = (\text{S}, \{B, C, D\})$

$\{B, C\} \geq \{B\}$

$\{B\} \geq \{B, C\}$

35

How many security labels can you build from the 4 hierarchal and five domain components? (Note, do not draw the lattice.)

$4 \times 2^5 = 4 \times 32 = 128 \text{ labels}$

What is the lowest upper bound (LUB) of the following labels (i.e., the lowest security label that dominates all labels):

$(\text{S}, \{A, C, E\})$
 $(\text{C}, \{A, B\})$
 $(\text{P}, \{\})$

LUB = $(\text{S}, \{A, B, C, E\})$

$\{A, C, E\} \cup \{A, B\} \cup \{\}$
 $= \{A, B, C, E\}$

What is the highest lower bound (HLB) of the following labels (i.e., the highest security label that is dominated by all labels):

$(\text{S}, \{A, C, E\})$
 $(\text{C}, \{A, B\})$
 $(\text{P}, \{\})$

HLB = $(\text{P}, \{\})$

$\{A, C, E\} \cap \{A, B\} \cap \{\}$
 $= \{\}$

empty set

(15 Points) Using the BLP rules and the security labels for John, Pete, Mary and the files above, fill out the following access control matrix with the read and write permissions. You can assume, that by default, anything not permitted is denied.

	File1	File2	File3	File4
John	r	r	r (deny read)	r (deny write)
Pete	r (deny read)	X	r	w (deny write)
Mary	w	w (deny read)	r, w	w

Assume that you want to enforce the following denials:

- Pete is not permitted to read File1 and he cannot write File 4.
- Mary cannot read File 2.
- John cannot read File 3 and cannot write File4.

Add the necessary negative permissions in the access control matrix if the BLP would permit the above actions for Pete, Mary, and John.

(10 Points)

After adding the denials for the users, did you get any conflicting permissions? List all the conflicts.

Pete \Rightarrow file 1, file 4
 John \Rightarrow file 3
 Mary \Rightarrow