

## Reading

Read Chapters 5 and 13 of *Access Control, Security, and Trust: A Logical Approach* (ACSTLA).

## Logistics

This homework is officially due in class on **Thursday, November 3**. However, it comes with an automatic (and longer than usual!) extension: anything submitted by **1pm on Friday, November 4** will be accepted as being on time.

**You may work singly or in pairs on this assignment:** if you work with someone else, turn in a single assignment with both names on it.

## Exercises

1. (22 points) ACSTLA, Exercise 5.4.1

*Note:* What I'm looking for is something akin to the example that appears at the top of page 94 (e.g., Figure 5.4), but you should include proofs for both the read and the write cases. You do not need to explicitly write out the derived rule, as it can be inferred from your proof.

2. (18 points) Consider the use of the standard military security levels (TS, S, C, UC), combined with categories (in this case, ENG, BUD, and PER). Thus the resulting security labels are given as follows:

$$\mathcal{L} = \{(t, X) \mid t \in \{\text{TS}, \text{S}, \text{C}, \text{UC}\}, X \in \mathcal{P}(\{\text{ENG}, \text{BUD}, \text{PER}\})\}.$$

The ordering on these labels is the standard *dom* ordering:

$$(t_1, X_1) \leq (t_2, X_2) \quad \text{iff} \quad (t_1 \leq_M t_2 \text{ and } X_1 \subseteq X_2),$$

where  $\leq_M$  is the standard military ordering ( $\text{UC} \leq_M \text{C} \leq_M \text{S} \leq_M \text{TS}$ ).

Finally, suppose the following security levels are assigned to the files  $A$ ,  $B$ , and  $C$ :

File	Level Assigned
A	(C, {PER, BUD})
B	(S, {ENG, BUD})
C	(S, {ENG})

For each of the following situations, give both the **highest** and the **lowest** security levels that would allow Willa to be given the indicated discretionary access, in accordance with the *Simple Security Condition* and the *\*-Property*. If no such level exists, explain why.

- (a) Discretionary **write** access to file  $A$  and discretionary **write** access to file  $B$
  - (b) Discretionary **read** access to file  $A$  and discretionary **write** access to file  $B$
  - (c) Discretionary **read** access to file  $A$  and discretionary **read** access to file  $C$
3. (40 points) ACSTLA, Exercise 13.2.3 (parts b, c, d)

*Note:* The intended interpretation of classification levels is that  $A \leq B \leq C \leq D$ .