6.8. Exercises

1:Prove Theorem 6–1 for the strict integrity policy of Biba's model.

2:Give an example that demonstrates that the integrity level of subjects decreases in Biba's low-water-mark policy. Under what conditions will the integrity level remain unchanged?

3:Suppose a system used the same labels for integrity levels and categories as for subject levels and categories. Under what conditions could one subject read an object? Write to an object?

4:In Pozzo and Gray's modification of LOCUS, what would be the effect of omitting the **run-untrusted** command? Do you think this enhances or degrades security?

5:Explain why the system controllers in Lipner's model need a clearance of (SL, { D, PC, PD, SD, T }).

6:Construct an access control matrix for the subjects and objects of Lipner's commercial model. The matrix will have entries for **r** (read) and **w** (write) rights. Show that this matrix is consistent with the requirements listed in Section 6.1.

7:Show how separation of duty is incorporated into Lipner's model. 7

8:In the Clark-Wilson model, must the TPs be executed serially, or can they be executed in parallel? If the former, why; if the latter, what constraints must be placed on their execution?

9:Prove that applying a sequence of transformation procedures to a system in a valid state results in the system being in a (possibly different) valid state.

10: The relations **certified** (see ER1) and **allowed** (see ER2) can be collapsed into a single relation. Please do so and state the new relation. Why doesn't the Clark-Wilson model do this?

11: Show that the enforcement rules of the Clark-Wilson model can emulate the Biba model.

12: One version of Polk's implementation of Clark-Wilson on UNIX systems requires transaction procedures to distinguish users in order to determine which CDIs the user may manipulate. This exercise asks you to explore the implementation issues in some detail.

a. Polk suggests using multiple copies of a single TP. Show, with examples, **exactly** how to set this up.

b. Polk suggests that wrappers (programs that perform checks and then invoke the appropriate TPs) could be used. Discuss, with examples, **exactly** how to set this up. In particular, what checks would the wrapper need to perform?

c. An alternative implementation would be to combine the TPs and wrappers into a single program. This new program would be a version of the TP that would perform the checks and then transform the CDIs. How dificult would such a combination be to implement? What would be its advantages and disadvantages compared with multiple copies of a single TP? Compared with the use of wrappers?

13: The text states that whether or not the integrity of a generic piece of software, or of generic data on which that generic software relies, has been compromised is undecidable. Prove that this is indeed the case.

13