2.8. Exercises

1:Consider a computer system with three users: Alice, Bob, and Cyndy. Alice owns the file **alicerc**, and Bob and Cyndy can read it. Cyndy can read and write Bob's file **bobrc**, but Alice can only read it. Only Cyndy can read and write her file **cyndyrc**. Assume that the owner of each of these files can execute it.

a. Create the corresponding access control matrix.

b. Cyndy gives Alice permission to read **cyndyrc**, and Alice removes Bob's ability to read **alicerc**. Show the new access control matrix.

2:In Miller and Baldwin's model (see Section 2.2.1), they restricted the functions that generated the access control matrix entries to working on objects, not on subjects. Thus, one could not base rights being granted on whether another subject possessed those rights. Why did they impose this restriction? Can you think of cases in which this restriction would cause problems?

3:The query-set-overlap mechanism requires a history of all queries to the database. Discuss the feasibility of this control. In particular, how will the size of the history affect the response of the mechanism.

4:Consider the set of rights {**read**, **write**, **execute**, **append**, **list**, **modify**, **own**}.

a. Using the syntax in Section 2.3, write a command **delete_all_rights** (**p**, **q**, **s**). This command causes **p** to delete all rights the subject **q** has over an object **s**.

b. Modify your command so that the deletion can occur only if **p** has **modify** rights over **s**.

c. Modify your command so that the deletion can occur only if **p** has **modify** rights over **s** and **q** does **not** have **own** rights over **s**.

5:Let **c** be a copy flag and let a computer system have the same rights as in Exercise 4.

a. Using the syntax in Section 2.3, write a command **copy_all_rights**(**p**, **q**, **s**) that copies all rights that **p** has over **s** to **q**.

b. Modify your command so that only those rights with an associated copy flag are copied. The new copy should **not** have the copy flag.

c. In part (b), what conceptually would be the effect of copying the copy flag along with the right?

6:This exercise asks you to consider the consequences of not applying the principle of attenuation of privilege to a computer system.

a. What are the consequences of not applying the principle at all? In particular, what is the maximal set of rights that subjects within the system can acquire (possibly with the cooperation of other subjects)?

b. Suppose attenuation of privilege applied only to **access** rights such as **read** and **write**, but not to rights such as **own** and **grant_rights**. Would this ameliorate the situation discussed in part (a)? Why or why not?

c. Consider a restricted form of attenuation, which works as follows. A subject **q** is attenuated by the maximal set of rights that **q**, or any of its ancestors, has. So, for example, if any ancestor of **q** has **r** permission over a file **f**, **q** can also **r f**. How does this affect the spread of rights throughout the access control matrix of the system? Develop an example matrix that includes the ancestor right, and illustrate your answer.