Information Assurance: Homework 6

Due October 26, 2009.

1. The following policy is enforced in a business:
    - Employees can access and update their own personal data. They can access their own salary information.
    - Managers can access personal and salary data about people that report to them
    - Managers can update salary information for people who report to them.

Consider a specific case with the following entities:

- Alice reports to Bob.
- Bob reports to Carol.
    a. Define the rights involved and create an Access Control Matrix to encode the protection state for this scenario.
    b. Write the following command in the HRU model make_manager(s1, s2) – Make s1 a manager of s2.
    c. Another rule is added to the policy. A manager can only change an employee's salary information if reviewed by their manager. Update the ACM to reflect the protection state with this new rule.
    d. Express the ACM as a set of access control lists.

2. In this question you will work through evaluating labeled access following the Bell-LaPadula confidentiality model and Strict Biba integrity model. For the first two sections consider the following labeled entities:

Subject	Object	Label
Alice	Plan1	L1
Bob	Plan2	L2
Carol	Plan3	L3
Dave	Plan4	L4
Ellen	Plan9	L5

The labels follow a complete ordering L1 > L2 > L3 > L4 > L5.

a. Interpret the labels as security labels in the simplified Bell-LaPadula model. Fill the the access column with the access that BLP would give each subject to the corresponding object: read, append (also mentioned in lecture as a pure write).

Subject	Object	Access?
Alice	Plan4	
Bob	Plan2	
Ellen	Plan3	
Dave	Plan9	

b. Now interpret the labels as integrity labels in the strict Biba model. Fill the access column with the access that strict Biba would give each subject to the corresponding object: read, write, execute.

Subject	Object	Access?
Alice	Plan4	
Bob	Plan2	
Ellen	Plan3	
Dave	Plan9	

c. Now consider the case where the labels have categories in addition to the completely ordered levels. We add categories alpha and omega. The new label assignments are:

Subject	**Subject Label**	**Object**	**Object Label**
Alice	L1:{alpha}	Plan1	L1:{alpha}
Bob	L2:{alpha,omega}	Plan2	L2:{omega}
Carol	L3:{omega}	Plan3	L3:{alpha, omega}
Dave	L4:{omega}	Plan4	L4:{alpha}
Ellen	L5:{alpha}	Plan9	L5:{omega}

Interpret these labels according to the Bell-LaPadula Model. Fill the the access column with the access that BLP would give each subject to the corresponding object: read, append (also mentioned in lecture as a pure write).

Subject	**Object**	**Access?**
Alice	Plan2	
Bob	Plan2	
Ellen	Plan4	
Dave	Plan9	

d. In class we only discussed the simple form of labels for Biba, but we mentioned the model could be extended to use the level and category labels as used in Bell-LaPadula. Now interpret the labels as integrity labels in the strict Biba model. Fill the access column with the access that strict Biba would give each subject to the corresponding object: read, write, execute.

Subject	**Object**	**Access?**
Alice	Plan2	
Bob	Plan2	
Ellen	Plan4	
Dave	Plan9	

3. Suppose a database for a department store contains an 'employee' table listing all employees' names, e-mail addresses, SSNs, salaries, hiring dates, and departments. The employee table rows for three employees is shown below

Name	Email	SSN	Salary	Hired	Department
Alice	alice@mart.com	xxx-xx-xxxx	$20.00	01/01/97	Appliance
Bob	bob@mart.com	yyy-yy-yyyy	$15.00	07/11/05	Shoes
Carol	carol@mart.com	zzz-zz-zzzz	$12.00	11/11/08	Hardware

a. Suppose you are the database administrator. Your company has a policy that each employee can see the names, e-mails, and hiring dates of all other employees in the same department. Show the SQL statements for these three employees to enforce this policy.

b. The company policy states that every employee should be able to view all fields about themselves in the 'employee' table. Show the SQL statements you would use to enforce this policy.

c. The company policy further states that an employee may choose to share this information with other employees of the company. How would you amend your answer in part b to enable an employee to allow other employees to view his or her non-public information in the 'employee' table?