Information Assurance: Homework 5

Due October 25, 2010

1. The following policy is enforced in a business:
    - Tellers can update customer balance data.
    - Auditors can review all customer data
    - Manager can approve the end of day balance review
    - Manager can create and close customer accounts

Consider a specific case with the following entities:

- Alice and Bob are tellers
- Carol is an auditor
- Dave and Ellen are managers
- Fred and Ginger are customers

a. Define the rights involved and create an Access Control Matrix to encode the protection state for this scenario.

b. Another rule is added to the policy. A teller cannot update their own balance data. Update the ACM to reflect the protection state with this new rule.

c. Express the ACM from part b as a set of access control lists.

d. Express the ACM from part b as a set of capabilities.

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

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

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 consider the case where the labels have categories in addition to the completely ordered levels. We add categories proj1 and proj2. The new label assignments are:

Subject	**Subject Label**	**Object**	**Object Label**
Alice	L1:{proj1}	Plan1	L1:{proj1}
Bob	L2:{proj1,proj2}	Plan2	L2:{proj2}
Carol	L3:{proj2}	Plan3	L3:{proj1, proj2}
Dave	L4:{proj2}	Plan4	L4:{proj1}
Ellen	L5:{proj1}	Plan9	L5:{proj2}

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	

3. Biba proposed three different integrity models.

a. In the Low water mark policy, the subject level potentially drops to eliminate indirect integrity problems through the information transfer path. Give an example of how the low water mark rules prevents low integrity data from propagating into high integrity data indirectly via the information transfer path.

b. In the Ring model, give an example of how low integrity data could be indirectly propagated via the information transfer path.

c. Does the strict Biba model solve the information transfer path integrity failure problem? Why or why not?

4. Suppose a database for a hospital contains an 'patient' table listing all patients' names, SSNs, diagnosis, assigned doctor, and notes. The patient table rows for three patients is shown below

Name	SSN	Diagnosis	Doctor	notes
Alice	xxx-xx-xxxx	pneumonia	Dr. Jones	
Bob	yyy-yy-yyyy	Broken leg	Dr. Jones	Change to walking cast
Carol	zzz-zz-zzzz	delivery	Dr. Smith	Induct by 7pm

In addition, there are employees.

- Nurses can read patient name, diagnosis and doctor. They should also be able to update notes.
- Doctors can read patient name. They can update diagnosis, doctor, and notes.
- Accountants can read name, ssn, and doctor.

Wendy is a nurse, Xavier is a doctor, and Zander is an accountant.

a. Suppose you are the database administrator responsible for enforcing the policies listed above. Show the SQL statements for these three employees to enforce this policy.

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