

Name:

## Information Assurance: Homework 2

Due September 8, 2006

1. The following policy is enforced in a clinic:

- Doctors can write prescriptions except for themselves.
- Nurses can review prescriptions.
- Pharmacists can fill prescriptions except for themselves.

Consider a specific case with the following entities:

- Drew is a doctor.
  - Cody and Carley are nurses.
  - Blair is a pharmacist.
  - Payton is a patient.
- 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. Nurse can write prescriptions if they are reviewed by a doctor who does not manage them. In the case above Drew manages Carley. Write another Access Control Matrix to encode the protection state with this new policy rule.

2. Consider the policies from the previous question. Write the following commands in the HRU model.

- a. `set_fill_right(s)` – Set the right to fill a prescription for the specified subject.
- b. `set_review_prescribe_right(n,d)` – Set the right to fill a prescription if reviewed by the specified doctor.

3. A portion of an acceptable use policy (AUP) states:

Students may not use University equipment for illegal or unethical purposes.

- a. Brady's account gets hacked, and spam is sent using her email account. Did Brady break policy?
- b. Before getting hacked, Brady posted her password and account information in her MySpace profile. Does this change your opinion of whether she broke policy?
- c. Instead of posting her account information, suppose that 60% of the accounts on the machine were hacked. Does this change your opinion of whether Brady broke policy?

Name:

4. Classify each of the following as mandatory or discretionary policy.
  - a. The room keying system in a dorm.
  - b. A next generation electronic room system in a dorm where the room inhabitants can give others access to their rooms.
  - c. A university registrar's office, in which a faculty member can see the grades of a particular student provided that the student has given written permission for the faculty member to see them.
  
5. Given the security levels: TOP SECRET > SECRET > CONFIDENTIAL > UNCLASSIFIED, and the categories A, B, and C, specify the accesses allowed (read, write, append) under the Bell-LaPadula model. Assume DAC allows all access.
  - a. Anna at CONFIDENTIAL:{C}. Document at CONFIDENTIAL:{A}
  - b. Paul at TOP SECRET:{A,C}. Document at SECRET:{A, C}
  - c. Robin at UNCLASSIFIED. Document at CONFIDENTIAL:{B,C}
  - d. Jesse at SECRET:{C}. Document at CONFIDENTIAL:{C}
  - e. Sammi at CONFIDENTIAL:{A}. Document at TOP SECRET:{A,C}
  
6. Consider the access allowed with the labels above under the strict Biba integrity model.
  - a. Anna at CONFIDENTIAL:{C}. Document at CONFIDENTIAL:{A}
  - b. Paul at TOP SECRET:{A,C}. Document at SECRET:{A, C}
  - c. Robin at UNCLASSIFIED. Document at CONFIDENTIAL:{B,C}
  - d. Jesse at SECRET:{C}. Document at CONFIDENTIAL:{C}
  - e. Sammi at CONFIDENTIAL:{A}. Document at TOP SECRET:{A,C}
  
7. Declassification effectively violates the \*-property of the Bell-LaPadula model. Would raising the classification of an object violate any properties of the model? Why or why not?
  
8. Suppose a system implementing Biba's model (the strict integrity policy) used the same labels for integrity levels and categories as for security levels and categories. Under what conditions could one subject read an object? Write to an object?
  
9. Explain why the system controllers in Lipner's model (discussed in section 6.3 of the book) need a clearance of (SL, {D, PC, PD, SD, T}).
  
10. Show that the enforcement rules of the Clark-Wilson model can emulate the strict Biba model.