

## Information Assurance: Homework 2 – Comments on Answers

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.

*W = write prescriptions for*

*R = review prescriptions for*

*F = fill prescriptions for*

	<i>Drew</i>	<i>Cody</i>	<i>Carley</i>	<i>Blair</i>	<i>Payton</i>
<i>Drew</i>		<i>W</i>	<i>W</i>	<i>W</i>	<i>W</i>
<i>Cody</i>	<i>R</i>	<i>R</i>	<i>R</i>	<i>R</i>	<i>R</i>
<i>Carley</i>	<i>R</i>	<i>R</i>	<i>R</i>	<i>R</i>	<i>R</i>
<i>Blair</i>	<i>F</i>	<i>F</i>	<i>F</i>		<i>F</i>
<i>Payton</i>					

*Most people got this part right. Some people tried to solve the problem with using Prescriptions as the object. But with that solution it is difficult to specify self restriction for doctors and pharmacists.*

*A couple people also added objects for the roles and added an “isa” right. This enables you to encode the role each subject holds in the 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.

*W = write prescriptions for*

*R = review prescriptions for*

*F = fill prescriptions for*  
*M=manage*  
*N(x) = write with review by x*

	<i>Drew</i>	<i>Cody</i>	<i>Carley</i>	<i>Blair</i>	<i>Payton</i>
<i>Drew</i>		<i>W, R</i>	<i>W,M</i>	<i>W</i>	<i>W</i>
<i>Cody</i>	<i>R, N(drew)</i>	<i>R, N(drew)</i>	<i>R, N(drew)</i>	<i>R,N(drew)</i>	<i>R, N(drew)</i>
<i>Carley</i>	<i>R</i>	<i>R</i>	<i>R</i>	<i>R</i>	<i>R</i>
<i>Blair</i>	<i>F</i>	<i>F</i>	<i>F</i>		<i>F</i>
<i>Payton</i>					

*Most people did not distinguish between the W right of Drew and the W right of Cody. In this solution, by having an approved write right that is specialized for the reviewing doctor, we can directly encode from the right in  $A[Cody,Payton]$  that she can write a prescription and the specific conditions that apply.*

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.

```

set_fill_right(s)
  for all o in O
    if o != s
      enter f into a[s,o]

```

- or -

```

set_fill_right(s,o)
  if o!=s
    enter f into a[s,o]

```

*I messed up here by not specifying an object parameter in the question. You either needed to add an object parameter or enumerate all objects. To be more stringent you could test to make sure that s is a pharmacist.*

- b. `set_review_prescribe_right(n,d)` – Set the right to fill a prescription if reviewed by the specified doctor.
- Similar issue with needing to specify the object as in part a.*

```

set_review_prescribe_right(n,d,o)
  enter N(d) into a[n,o]
  if m in a[d,n]
    delete N(d) from a[n,o]

```

*HRU does not allow for negative conditional checks. This is one trick to get around this limitation. Another trick would be to create a temporary object, associate rights with it and conditionally delete it.*

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?

*No, Brady did not use the system unethically*

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?

*This one could be argued both ways. Very strictly speaking she was not using the equipment directly when posting her password information. However, upon review most reasonable people would say that she had acted to directly to enable others to use the equipment unethically and had implicitly given her consent. To make the matter clearer the AUP should also say something about keeping account information private.*

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?

*Brady is not breaking the policy, again, Brady is not using the system unethically.*

4. Classify each of the following as mandatory or discretionary policy.  
*In each of the cases below, if you gave a good argument for the other point of view I awarded at least partial credit.*
- a. The room keying system in a dorm.
    - i. *Mandatory. Normally you cannot duplicate keys. The key is associated with the student and assigned by the powers that be.*
  - b. A next generation electronic room system in a dorm where the room inhabitants can give others access to their rooms.
    - i. *Discretionary. The inhabitants have discretion on who to give access.*
  - 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.
    - i. *Discretionary. At least with respect to the students. The faculty have no control over the access. And the students themselves only have limited control to allow the class of faculty members not the university population at large.*
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.  
*Note: I am treating append as writing up. Write is assumed to be both a read and a write.*
- a. Anna at CONFIDENTIAL:{C}. Document at CONFIDENTIAL:{A}
    - i. *none. Confidential:{C} and Confidential:{A} are not comparable. One does not dominate the other.*
  - b. Paul at TOP SECRET:{A,C}. Document at SECRET:{A, C}
    - i. *read. TOP SECRET:{A,C} dominates SECRET:{A,C} so the simple security condition holds.*
  - c. Robin at UNCLASSIFIED. Document at CONFIDENTIAL:{B,C}
    - i. *append, CONFIDENTIAL:{B,C} dominates UNCLASSIFIED:{} so the \*-property holds.*
  - d. Jesse at SECRET:{C}. Document at CONFIDENTIAL:{C}
    - i. *read, SECRET:{C} dominates CONFIDENTIAL:{C} so the simple security condition holds.*
  - e. Sammi at CONFIDENTIAL:{A}. Document at TOP SECRET:{A,C}
    - i. *append, TOP SECRET:{A,C} dominates CONFIDENTIAL:{A} so the \*-property holds.*
6. Consider the access allowed with the labels above under the strict Biba integrity model.

Similarly here I was assuming that people would be using read, write, and append with the same meanings as in question 5. Some people used write and execute instead. If you clarified your assumptions, I gave credit.

- a. Anna at CONFIDENTIAL: {C}. Document at CONFIDENTIAL: {A}
    - i. none, the labels are incomparable.
  - b. Paul at TOP SECRET: {A,C}. Document at SECRET: {A, C}
    - i. append, TOP SECRET: {A,C} dominates SECRET: {A,C} so the integrity version of the \*-property holds.
  - c. Robin at UNCLASSIFIED. Document at CONFIDENTIAL: {B,C}
    - i. read, CONFIDENTIAL: {B,C} dominates UNCLASSIFIED: {} so the integrity version of the simple security condition holds.
  - d. Jesse at SECRET: {C}. Document at CONFIDENTIAL: {C}
    - i. append, SECRET: {C} dominates CONFIDENTIAL: {C} so the integrity version of the \*-property holds.
  - e. Sammi at CONFIDENTIAL: {A}. Document at TOP SECRET: {A,C}
    - i. read, TOP SECRET: {A,C} dominates CONFIDENTIAL: {A} so the integrity version of the simple security condition holds.
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?
- a. No. writing up is allowed, by raising the classification level you are simply removing read access from people who were at the original classification level.
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?
- a. Subject can read and write if and only if the objects are at the same levels. I.e., Anna at confidential: {a} can only read and write objects that are also confidential: {a}.
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}).
- a. System controllers need to be able to read development code and write production code. They, however, do not need to read the logs or anything to do this hence they aren't AM...

*Note: Many people did not explain why System Controllers did not have AM. This resulted in partial credit*

10. Show that the enforcement rules of the Clark-Wilson model can emulate the strict Biba model.

- a. *Imagine you have 3 integrity levels, H, M and L. You could define a total of 9 TPs:  $TP_{H\_read}$ ,  $TP_{M\_read}$ ,  $TP_{L\_read}$ ,  $TP_{H\_write}$ ,  $TP_{M\_write}$ ,  $TP_{L\_write}$ ,  $TP_{H\_exec}$ ,  $TP_{M\_exec}$ ,  $TP_{L\_exec}$ . Then, according to ER2 you should define a set of allowed relations. Users with integrity level H should be assigned  $TP_{H\_read}$  for all data at or above their level,  $TP_{H\_write}$ , for all data at or below their level, and  $TP_{H\_exec}$  for data at or below their level. Similar for users with integrity level M and L. ER3 ensures users are how they say they are and ER4 ensures that users cannot artificially give themselves access to data they shouldn't see. It is in this way that C-W can emulate Biba.*