CS 290C – Spring 2013 – Homework Assignment 3

Due Thursday, May 30th

Do not discuss the problems with anyone other than the instructor.

Submission Instructions: For the first problem you can turn in either a hard copy or a pdf file. For the second problem turn in the Alloy specifications and the output generated by the Alloy Analyzer in separate files. Include a readme file to explain your solutions if necessary. Email the zipped directory containing your solutions (subject line: 290C HW3).

1. Consider the following specification for a web application:

This web application allows students to add and drop courses. Each course has a name and a number. Each course is taught by one professor and is taken by one or more students. Each professor has a name. Each student has a name and a perm number. Each student is either a graduate or an undergraduate student.

From the home page a student can search a course by entering a description in a form. The resulting page lists the courses that match the description. The student can choose a course from the list and go to the course add page that lists the information about the course and the professor who teaches the course. In the course add page there is a link that enables the student to confirm the add and go back to the home page.

From the home page, student can follow a link to see the current courses he is enrolled in. Student can choose a course from the list and go to the course drop page. In this course drop page there is a link that enables the student to confirm the drop and go back to the home page.

(a) Specify the data model for this Web application as a class diagram (like the entity-relationship diagrams in WebML).

(b) Specify the navigation model for this specification in WebML. (In the navigation model, instead of using the visual notation for the content and operation units, you can use their names from Tables 1 and 2 of the "Conceptual Modeling of Data-Intensive Web Applications" paper).

2. This problem is about modeling role based access control policies for a health-records website. There are three roles: patient, doctor and administrator. There are two resources: health-record and medical-bill. Each health-record and medical-bill are associated with a single patient and each patient has a single health-record and zero or one medical-bills. Each health-record is associated with one or more doctors and one or more administrators. Each medical-bill is associated with one or more administrators.

Here are two access control policies for this site:

- Policy-1: Each patient can access to his/her own health-record and medical-bill. Each doctor can access to the health-record's that he/she is associated with. Each administrator can access the health-records and medical-bills that he/she is associated with.

- Policy-2: Each patient can access to his/her own health-record and medical-bill. Each doctor can access to all health-records. Each administrator can access the health-records and medical-bills that he/she is associated with.

Model these access control policies in Alloy as follows: First create sigs for user, patient, doctor, administrator (where patient, doctor and administrator are subsets of user), resource, health-record and medical-bill (where health-record and medical-bill are subsets of resource) and the associations among them. Then write predicates called access-resource that take a user and a resource as input and return true based on the access control policy. Write these predicates for both policies mentioned above.

Show that Policy-1 is more strict than Policy-2 using the Alloy Analyzer.

Check if the following properties hold on these access control policies using the Alloy Analyzer: 1) A doctor cannot access to a patient's medical-bill. 2) A patient can only access to his/her own health-record. 3) An administrator cannot access to any health-record or medical-bill that he/she is not associated with.

If the above properties do not hold, then refine the above policies or the properties so that they hold.