CS6133 Course Project

For this course project, you will write two model specifications for a small software system and verify the each specification satisfies certain desired properties. The project has been designed to allow you to apply the formal techniques and tools discussed in class to the problems of specifying and validating a software system.

You will work in groups of size two. The course project has two deliverables, including a comprehensive report as well as the specification code in terms of the input languages to the tools you select to employ. The report will document the design of system, a short tutorial of the tool you choose to employ, the verification results you have obtained, and the experience you have gained.

First, you will verify the small software system using NuSMV. Second, you choose one of the tools from SPIN, Alloy, JavaPathFinder, and Beaver. You are responsible for downloading the tool, exploring the tool, and gaining hands-on experience with the tool.

Possible software systems that you can choose to verify include

1. An elevator control system (See enclosed description)

2. A privacy policy enforcement system (See enclosed description)

3. A non-trivial software/hardware system related to your research.

The deliverables shall be sent to Jianwei Niu via email by May 8, 2014. Every group will demonstrate the project on May 8, 6 pm – 8:00 pm.

I. An elevator control system

You will specify the behavior of a software system to be installed to control a simple elevator system. The elevator services a three-floor building. Inside the elevator there are request buttons, one for each floor. If the user inside the elevator presses a button, the elevator will visit the corresponding floor and open its doors. Floor 1 and floor 3 each has a request button that a user presses to command the elevator to come to that floor and to open its doors. Floor 2 has two request buttons to indicate which direction (up or down) the user will want to be taken once they are inside the elevator. If the elevator's doors open, they should stay open for five time units. The elevator has two buttons to open and close the doors. When any of these buttons is pressed, the button will light up until the request is responded. You should not make any assumptions about how much time it takes the elevator to move between floors.

At the very least, you should make sure that the following properties hold in your system with the help of a verification tool.

1. Requests to be delivered to a particular floor are eventually serviced
2. The elevator never moves with its doors open

II. A privacy policy specification and enforcement system

Healthcare organizations that gather and use private information are required to provide assurances that their information systems meet organizational and regulatory privacy-policy requirements. Privacy requirements are complex, as are the information systems that must meet them. The need for techniques and tools that provide a much stronger basis for ensuring electronic information systems do their part in enforcing privacy policies is strong. In this project, the privacy policy we aim to verify and enforce is expressed in temporal logic. It captures not only safety, but also liveness requirements, which are essential in privacy policy. You will develop a usable formal technique to specify a security and the privacy policy and verify that that policy you create complies with Health Insurance Portability and Accountability Act (HIPAA) rules.