

## CS6133 Course Project

For this course project, you will write a model specification for a small software system and verify the 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 four or five. The course project has two deliverables, including a comprehensive report as well as the specification code in terms of the input language to the tool you select to employ. The report will document the design of system, a tutorial of the tool you choose to employ, the verification results you have obtained, and the experience you have gained.

Tools that recommended for the use in the project include SPIN, JavaPathFinder, Bandera, BMC, Beaver, UPPAAL, and Concurrency Workbench. You are responsible for selecting one tool from the list, downloading the tool, and exploring the tool, and gaining hands-on experience with the tool. You may also develop your own model checkers or SAT solvers. Moreover, you may investigate or develop verification techniques that deal with large or infinite state systems.

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 Dec. 12, 2011. Every group will demonstrate the course project on Dec. 10, 5:30 pm – 8:30 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 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. There is the need for techniques and tools that provide a much stronger basis for ensuring electronic information systems do their part in enforcing privacy policies. In this project, the privacy policy we aim to enforce is expressed in restricted first-order temporal logic (FOTL) [1][2]. It captures not only safety, but also liveness requirements, which are essential in privacy policy.

In this project, you will develop a policy analysis technique (e.g., semi-decision procedures) to ensure that the Health Insurance Portability and Accountability Act (HIPAA) specified in terms of CI can be incrementally monitored or enforced by a message-passing based medical information system.

1. Adam Barth, Anupam Datta, John C. Mitchell, and Helen Nissenbaum. "Privacy and contextual integrity: Framework and applications". Proceedings of the 2006 IEEE Symposium on Security and Privacy, pages 184–198, 2006.
2. Deepak Garg, Liming Jia, and Anupam Datta. "Privacy Auditing over Incomplete Logs: Theory, Implementation and Application", Proceedings of the 18<sup>th</sup> ACM Conference on Computer and Communications Security, 2011.