

Term Project

Why a Project?

This course covers a very large discipline, and—perhaps more so than many other areas of computer science—the discipline of computer security runs through many other areas. Because the class has a very limited amount of time, we will only touch the surface of many topics. The project is to give you an opportunity to explore one of these topics, or some other area or application of computer security that interests you, in some depth.

The Ground Rules

The project can be a detailed research paper or survey, or a programming project that focuses on validating or working with some formalism or implements a model so others can explore it thoroughly. It can be a formalism, a model, or something else theoretical that we do not cover in class. In any case, check with me before beginning to be sure it is a reasonable project and no-one else has chosen it. Please select something that interests you!

You may work individually, or in groups of up to 3 people (if you want to have more than 3, please come see me). Of course, the larger the group, the more I will expect from it.

Some Suggestions for Project and Report Topics

Below are some suggestions for projects. If you pick one of these, you will need to refine it or limit the scope of your project. I also encourage you to think of a project on your own, especially in an area of computer science, or its application, that interests you.

- Develop a model of information flow through a network using the Take-Grant Protection Model, and demonstrate its utility by analyzing a situation of your choosing.
- Find a high assurance system (such as GEMSOS) that implements a security policy model. Explain in detail how the system instantiates the policy.
- Present a survey of confidentiality models other than the Bell-LaPadula Model.
- Analyze an existing digital rights management scheme, suggest improvements, and show how your suggestions improve the ability of the modified scheme to meet its requirements.
- Develop and apply a model of availability to a system or some other entity.
- Examine the composition problem, and focus on advances in the nature of composition and restrictiveness.
- Insert information flow analysis into a compiler or assembler and use it to detect flows that violate a policy specifying security/integrity levels for a program or system.
- Build a run-time system that detects flows that violate a policy specifying security or integrity levels for a program or system.
- Develop a covert channel or side channel analyzing tool and use it to analyze a subsystem or some other entity.
- Develop a formalism or model for analyzing some aspect of the “insider problem”.
- Create a model for a specific problem, such as electronic voting, and use it to reason about properties of the desired systems.

What Is Due and When

Please submit the following on the dates indicated:

1. *Project selection*: due on Friday, January 22; 10% of project score. Submit a write-up with your team members consisting of a one-line title of your project, a one-paragraph description, and the names of all team members. If you're doing a programming project, state the problem you want to solve and the requirements for a solution.
2. *Progress report*: due on Friday, February 12; 20% of project score. Submit a one-page progress report, and a bibliography of references that you have used or plan to use.
3. *Completed project*: due on Friday, March 18 **no later than 3:00pm Pacific time (no extensions can be given)**; this is the date and time of the final exam, which ends at 3:00pm; 70% of your project score. Turn in your final project. Submit these to the class site in Canvas as described in **All About Homework**. If a team has multiple members, only one need submit the material. The others are to submit a note saying who submitted the material (a one-line text file is fine for this).