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

You may select a project from the list below (in most cases, you will need to refine or limit the suggestions). You may also think of a project on your own. The project can be a detailed research report or survey, or a programming project. 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 4 people (if you want to have more than 4, please come see me). Of course, the larger the group, the more we will expect from it!

Some Suggestions for Project and Report Topics

* Handling phishing attacks, spam, and other annoying mail
* Security requirements for a specific environment, such as a medical environment or an academic research environment
* Given a security policy, how can you automatically configure systems to enforce that policy?
* Given a system or set of systems, how can you automatically generate a description of the security policy it enforces?
* Factoring a number
* Designing and implementing a firewall with specific properties and features
* Elections, electronic voting machines, and computer security
* Modifying access control mechanisms to an existing system (for example, adding rings or capabilities to Linux or Windows)
* Rights and amplification of rights in a capability-based system
* Standards for secure electronic communications (like electronic mail or chat tools). This includes the security properties and options of IP version 6, SSL, ATM, or some other protocol(s).
* Designing a program (or set of programs) to apply statistical analysis to ciphers (you will have to narrow this down *a great deal!*)
* Source code analysis of an open-source project or tool for which source code is available
* Handling intrusions: detection, tolerance, response (the last two are very hot topics right now!)
* Develop and implement a large (useful) program using assurance techniques, and argue convincingly why it is "secure" (mail server, WWW server, etc.)
* Analyzing a system's or site's security.
* Developing a security tool (you can pick what you want to write, but please check with me first!)
* Attacking systems; how, who, why, and so forth

What is Due, When

Please submit the following on the dates indicated:

1. ***Project selection***: due on Friday, January 13; 10% of project score. Submit a web page with your team members, a one-line title of your project, and a one-paragraph description. If you're doing a programming project, state the problem you want to solve and the requirements for a solution. A template for the web page will be available on January 9 on MyUCDavis.

2. ***Project due***: due on Wednesday, March 18 (this is the last day of class); 90% of your project score. Turn in your final project.

In all cases, submit the project to MyUCDavis as described in **All About Homework**. If a team has multiple members, only one need submit the material, and the others can simply submit a note saying who submitted the final project.