Projects

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 gives you an opportunity to explore one of these topics, or some other area or application of computer security that interests you, in some depth.

Suggestions for How to Proceed

First, choose a topic. Good ways to find a topic are to think about an area of computer science you enjoy, and try to relate it to computer security (or vice versa); talk to some other graduate students and see if what they are doing suggests any ideas; think of ways security of the system you're working on could be made better; go to the library and browse for an interesting-looking paper; and so forth. The major computer security journals are *Computers & Security* and *Journal of Computer Security,* but articles appear in almost all journals; the major conferences are *Crypto* and *Eurocrypt* (for cryptography), *Symposium on Research in Security and Privacy, National Computer Security Conference*, and the *Annual Computer Security Applications Conference.* If you need more help or have questions, feel free to talk to me.
This term, you may also use the penetration study as your project (see below). If you do this, you will need to turn in a final report as well as the interim reports and presentations (if you are not on campus, don't worry about the presentations).

Some Suggestions for Project and Report Topics

- Biology and Computer Security: viruses, worms, and so forth
- The Adoption of the DES
- Security Requirements in Educational, Commercial and Governmental Environments
- User/System Authentication Methods
- Formal Models (for example, something in depth on HRU, TPM, etc.)
- A Study of the Security of the *your.favorite.operating.system* System (check with me on this one!)
- Property-based Testing
- Electronic Voting Machines and Computer Security
- Rights and Amplification of Rights in a Capability System
- How the Attackers Do It
- Auditing and Logging
- Breaking Ciphers with Computers (you will have to narrow this down a *great deal*)

What Is Due When

Friday, April 25	By this time you should have chosen your project. Turn in a 2–3 page writeup of what you want to do, and why; list several sources, and describe how you plan to go about completing the project. For example, if you are writing a survey paper, state the theme and in general terms how you will organize your paper.
Wednesday, May 14	By this time your project should be well underway. Turn in a 3–4 page description of what you have done, approaches that you took and that failed, and so forth. For example, for a survey paper, turn in a brief description of what your references contain, and present a detailed outline of your paper.
Friday, June 6	Your completed project is due.

#	Date	Topic, Readings, and Other Information
25.	Monday, May 26	***Memorial Day — University Holiday***
26.	Wednesday, May 28	Access Control Mechanisms (con't) Mandatory and Discretionary Controls, Origination Control
27.	Friday, May 30	Security Kernels Principles, trusted path, covert channels, principle of layering, verification; discussion of examples *Reading*: *text*