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

*   Malicious logic and biology: how computer worms, viruses, *etc.* compare to their biological counterparts
*   Security requirements in an academic environment (or another environment; medical environments are a hot topic right now)
*   Automating policy checking (to ensure your computer/site meets a given policy) and/or definition
*   Authenticating users and systems (especially over untrusted networks)
*   Factoring a number
*   Design and implement a firewall with specific properties and features
*   Electronic voting machines and computer security (this is a very hot topic right now)
*   Modifying access control mechanisms to the UNIX, Windows, or Macintosh system (for example, adding rings or capabilities)
*   Rights and amplification of rights in a capability-based system
*   Secure electronic mail: proposed standards
*   Design a program (or set of programs) to break a cipher; for example, a cryptographers' toolkit (you will have to narrow this down a *great deal*)
*   Analyzing and/or testing programs for vulnerabilities (pick a couple as examples)
*   Intrusion detection and incident response (incident response is another very hot area right now)
*   Write a large (useful) program using the techniques we discussed in class, and argue convincingly why it is "secure" (mail server, WWW server, *etc.*; these may have limited functionality)
*   Analyzing a system's or site's security. Be sure you have *written permission from the appropriate people first!*
*   Security features of IP version 6 (or ATM, or SSL, or another protocol): how good are they?
*   Comparing Windows NT security tools and UNIX security tools (with respect to functionality, assurance, *etc.*)
*   Developing a security tool (you can pick what you want to write, but please check with me first!)
*   User interfaces to security tools or configuration mechanisms; do they help or hurt the security of the system? How could they be made better? How well do they work now?
*   Attacking systems; how, who, why, and so forth

What Is Due

1. Project selection: *due date*: October 8, 2003; *weight*: 10% of project score
    Submit a one-line title for your project, a list of team members and their email addresses, and a short (one paragraph) description that explicitly states the goal of your project. Please submit only one write-up for your team!
2. Project: *due date*: December 5, 2003; *weight*: 90% of project score
    Submit your completed project. Please be sure the submission names *all* team members!

In all cases, submit the project to *MyUCDavis* as described in **All About Homework**.