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 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. The specific goal of the project is to produce a paper. The paper may document software (or hardware) work, so you may choose that kind of project. The paper must either be of publishable quality, or be publishable should some (small amount) of additional work be done. You are free to work singly or in groups. Groups should have between 2 and 4 people; if you want to have more than 4, please check with me *first*.

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*, the *Journal of Computer Security* and the *ACM Transactions on Information and System Security,* but articles appear in almost all journals; the major conferences are *Crypto* and *Eurocrypt* (for cryptography), the *IEEE Symposium on Research in Security and Privacy*, the *National Computer Security Conference* (also known as the *National Information System Security Conference*), and the *Annual Computer Security Applications Conference.* If you need more help or have questions, feel free to talk to me.

Some Suggestions for Project and Report Topics

The following are just to get you thinking. You will need to do much refinement for each!

- Analyze your favorite Internet or network protocol with respect to specific security requirements. Is it adequate, or should changes be made to enhance its ability to meet stated goals?
- UC Davis has an electronic mail security policy. Is it reasonable or realistic? What are the legal implications? Could you improve it from the point of view of system administration?
- Look at attack signatures and derive a little language to capture some class of them. Can you generalize your language to include as many attacks as possible? Focus on the temporal aspects.
- Add temporal logic to the Take-Grant Protection Model.
- The non-interference and non-deducibility results are related to multi-level security used to protect confidentiality. Can you either extend those results to the Biba integrity model, or set up a similar notion for integrity-based or availability-based models?
- How would you look for non-secure settings of environment variables in an executing program? Can you develop a wrapper that will check those values whenever a subprocess is spawned? (The motive here is that we may not have access to the source code, but can wrap the program so when it executes, the wrapper controls execution and can stop the wrapped program to check state.) You may need to hack a kernel to do this.
- Pick a class of vulnerabilities, analyze it, and design tools to check for those problems in program. Substantiate any claims of success by implementing a prototype and using it.
- Take a popular security tool and improve it by adding to it, simplifying the user interface, or in some other fashion. Support your claim of having improved it with some tests to demonstrate the new tool does work better.
- *Or whatever you think you will find interesting ...*

What Is Due When

All submissions are to be made through MyUCDavis.

Tuesday, April 13   By this time you should have chosen your project. Turn in a 2–3 paragraph write-up of

what you want to do, and why; list several sources (at least 3), and describe how you plan to go about completing the project.

Tuesday, June 8   Your completed project is due.