Computer Sciences, UW–Madison
CS 838: Computer Security
Course Syllabus

Fall 2013
Instructor: Thomas Ristenpart
September 3, 2013

Course Information

Meets: Monday, Wednesday, Friday, 9:30PM–10:45PM in CS 1263. We'll typically meet 2 days a week, most often M/W.

Instructor: Thomas Ristenpart

Office: 7387 Computer Sciences

E-mail: rist@cs.wisc.edu

Course Web Page: `http://pages.cs.wisc.edu/~rist/838-fall-2013/`. Announcements and reading list will be posted there.

Contents: This course will be an introduction to research in computer security. We will cover a wide range of topics, ranging across software security, web security, e-crime, cryptography, embedded system security, and more. The goal will be to introduce students to, and prepare them to conduct, computer security research. As such the course will focus on reading, evaluating, and discussing papers as well as two projects.

Paper reviewing: We will target understanding two (perhaps sometimes three) papers a week. For each paper, at least two students will be assigned as *reviewers* and more often three. That means they will be responsible for writing a short summary and evaluation of the paper. The summary must be prepared without collaborating with the other reviewer(s) assigned to the paper. (You may discuss the paper with other classmates, as long as those classmates are not also discussing it with the other reviewer. Any classmate who helped in preparation of your summary, including myself, should be explicitly acknowledged in the summary.)

The summary must be prepared using Latex, and in particular use the Latex template that will be made available on the course webpage.

The summary must be *finished at noon the day before the class*. The summaries will then be made available to the rest of the class.

There are about 15 weeks of class, and so we'll probably have around 30 papers. Assuming 15 are enrolled and 3 reviewers per paper, each student will review 6 papers in the course of the semester. This is just an estimate, and you will know soon how many papers you'll be responsible for and when (see reviewer assignments below).

The goals of the summaries are several-fold. First, to gain experience evaluating and understanding research papers and see how independent reviewing can lead to different conclusions about papers. Second, to help your classmates, who want to understand the papers at least as well as you (the reviewer) do. Third, to ensure high-quality discussions. Fourth, to crowd-source a study guide for an eventual qualifier in security.

Class discussion: Lectures will be largely dedicated to in-depth discussion of papers. For each paper, we will start with one of the reviewers (picked at random during class) to verbally summarize the paper. Both reviewers therefore need to be at class (see below regarding what to do if you will miss a class). Use of a chalkboard is fine, but slides are discouraged.

All students are expected to be familiar with the papers and participate in discussion, even if the discussion topics are initiated by the reviewers. That means reading the papers for the class that day, and reading the summaries submitted by the reviewers.

We will discuss the paper, expanding on the evaluations given by the reviewers, and (most importantly) identify further open problems and discuss them. Should it be necessary, I will arbitrarily pick one of the reviewers of a paper to be its *shepherd* and ensure that all evaluations are updated to reflect the discussion.

Paper list and reviewer assignments: I've started putting together a list of papers, and the schedule for a few weeks is up on the web page. I have a set of topics in mind I think we will fill the rest of the time with, but I want to leave this in large part up to you. Security is broad and there is no hope we can cover everything that is of interest. Your first assignment is to add to the brainstorming list papers you are interested in incorporating into the reading list. You can add as many as you want (within reason), but I expect everyone to add at least one. Sources of interesting papers are your own ongoing research interests, top conferences in security or cryptography (for security: IEEE Oakland Symposium on Security and Privacy, ACM Computer and Communications Security, USENIX Security, ISOC Networked and Distributed Systems Security; and for cryptography: Crypto, Eurocrypt, Asiacrypt), or even non-security venues (for example, new architectures, systems, or network designs often are ripe for security analysis, and are in-scope). This is due on Friday. I'll release a final schedule at the end of the weekend.

I will randomly assign reviewers to each paper, and besides the first week you should have plenty of lead time. Students are allowed to swap review assignments as they please, so long as both parties agree, and it is recorded with me ahead of the due date/time. If something comes up and you are unable to review a paper and can't find someone to swap with, then email me and we'll figure something out.

Projects: The other large component of the class will be two research projects. These can be done either individually or in groups, and the groups must stay the same for the two projects. Projects that dovetail with other classes or ongoing research projects with non-class collaborators will be allowed, though you will need to explain your role (and have that be commesurate with doing a project on your own). The two projects are:

- *The pitch (due October 2)*: The first will be a short duration project to gain some basic skills and lay the groundwork for the main project. The pitch will culminate in a short (5–10 minute) presentation in class, a short accompanying write-up (a few latex'd pages), and any supporting datasets. The goal of the mini-project is to pitch the class on the potential value of the main research project. As such, it will focus on finding and justifying the problem that you propose a main project tackles.

- *Main project (due December 13)*: The final project will build on the pitch, including feedback on it. It will culminate in a short paper (prepared using latex). We'll either do a poster session

or presentations on the final projects. The project should be at the level of publishable (or laying the groundwork for) publishable research. The pitch will help in that process.

I'll discuss in class more details about the pitch and main project.

Grading: Grades will be assigned based on class participation (15%), quality of the reviews (40%), quality of the pitch (15%), and quality of the final project (40%). This is a graduate level course, and so I expect that effort and, consequently, grades will tend to be high.