CS 591 Spring 2008 - Computer Security and Privacy

Instructor: Jedidiah Crandall

Class Meeting Place and Time: Dane Smith Hall 134, 12 noon-12:50pm, MWF.

Web page: http://www.cs.unm.edu/~crandall/591spring08/

Required Text: (1) Either of Matt Bishop's books should be fine, the green undergrad version at the bookstore (Introduction to Computer Security), or the brown graduate version with the same content but more detail (Computer Security: Art and Science). Note that if I assign a chapter to read, the chapters in the brown book are usually about twice as long. (2) The Sciences of the Artificial by Herbert A. Simon (Third Edition).

Additional Readings: I will assign a lot of additional reading. I'll try to be explicit about what level of reading is necessary (skimming, reading most of it but skimming over particular parts, or reading carefully). If you try to read everything word-for-word the reading in this class will be overwhelming. We may sometimes split the reading (i.e., everyone skims all five papers, but student A reads paper #1 carefully, student B reads paper #2 carefully, etc.). Please provide feedback at any time during the course if the reading level gets too heavy and we'll adjust accordingly.

Prerequisites: No official prerequisites. Some of the material is very technical in nature, but I'll only assume that you have a Computer Science Bachelor's degree level understanding of operating systems, architecture, and networks.

Grading: The grade will be based 50% on your attendance and participation in class (including writeups/short essays that I ask for on particular papers and chapters) and 50% on an individual research project. No curve, so 80-85 is a B, 85-90 is a B+, 90-100 is an A, and anything below 80 is probably a B- or a failing grade (C).

The participation grade will be broken up into 10%, 20%, and 20% that I will assign a
few weeks into class, mid-semester, and at the end of the semester, respectively.

The project grade will be broken up into a proposal (5%), three short interim reports (5% each), a final paper (20%), and a final presentation (10%).

**Cheating and Collaboration:** Everything in this class, including small writeups I ask for and all deliverables and work for the final project, are to be individual efforts unless I specify otherwise.

**Homework:** I'll assign light, informal assignments (e-mail me your thoughts, write a few paragraphs about such-and-such, etc.) that won't be officially graded, but will factor into your participation grade.

**Information About the Project**

The class project is an individual project and must encompass some original work, either in terms of implementation effort or mathematical formulation. There must also be some intellectual merit. In other words, no experience papers that have no academic merits, survey papers, or position papers. Duplication of results is encouraged, however, but talk to me if that's what you want to do (debunking one of my papers is a perfectly valid project).

Since it is difficult to come up with original research ideas at the beginning of the semester in an area that's new, I'll post some possible projects with intellectual merit that are related to my own research and you can propose to work on one of them if you choose (I certainly won't mind the free labor ;-). See the policy about credit below and make sure to come to me with any concerns whatsoever before, during, and after the project.

**Proposal:** Having an original research idea for the proposal is critical, obviously, but for your project in this class it doesn't matter whether you came up with it or whether it's an idea from your advisor or myself that you are interested in working on. What will matter
for the proposal is that in 1-page maximum, NSF-compliant format (all margins at least 1", maximum 10 point font, no more than six lines of text in an inch), you are able to convince me that the work you propose to do (a) has intellectual merits, (b) has broader impacts, (c) can be done in a 3-credit-hour load over a single semester, and (d) that you're the right person to do it (include references to any relevant past coursework or research). I strongly recommend that you work with me and bounce a draft or two off of me before the proposal is due. Be sure to discuss with me beforehand any overlap between the work you propose and any research you are doing with your advisor or that you are doing as a project for another class.

**Interim Reports:** I expect that you'll work on this project throughout the semester and put significant effort into it, which is why I strongly recommend that you choose a project that you are very, very interested in. The interim reports are my way of making sure you're not waiting until the last week of school to throw some code together, generate some half-baked results, and turd-polish it into an interesting-enough read that the instructor gives you brownie points for at least not being totally incompetent at writing. I became an expert at this at U.C. Davis, but I won't let you get away with it.

**Final Paper:** In 2-column, 10pt font write a conference-submission-style research paper, 10 page maximum. I'll grade it on the same criteria as a reviewer would.

**Final Presentation:** These will probably be about 15-20 minutes, the grading criteria being how interested the average CCS/Oakland/USENIX Security conference attendee would be in reading your paper after having seen the presentation.

**Publication Credit and Software:** If you want to work on a project that fits into my research agenda, *e.g.*, developing a Good-Turing estimator for our Great Firewall of China blacklist or doing a Wray-style timing channel analysis of a virtual machine, that is great but it doesn't guarantee that I'll be able to support you as an RA in the future and we need to be careful about my ability to work on the same topic in the future and give any due credit. In general, I consider intellectual contributions to be worthy of authorship on any paper, and source code implementation not so much, but I can be pretty flexible about such things. I just want to avoid situations where credit attribution
is ambiguous (credit attribution means whether 591 student is the first author, second author, cited in the acknowledgments, etc.), such as the following examples:

* A 591 student takes on one of my research ideas and develops a Good-Turing estimator that is not so good. Then later one of my RAs develops one that is publishable.
* A 591 student writes source code to inject malware into a VM environment and then one of my research students uses the code to do something very novel.
* A 591 student makes an observation that could be viewed either as an obvious statement of what anyone would think or as a truly insightful intellectual contribution, depending on who you ask. E.g., "You should probe for IPv6 routes as well," in a context where I had already been planning to do so.

I'd be very happy to have 591 students work on either my malware analysis or censorship research, but we have to be careful. My policy is:

1. Authorship is for people who contributed novel intellectual insights, or made an exceptional implementation effort that is central to the paper, and the first author (unless the paper is theoretical and alphabetical order is more appropriate) is the student who contributed the most.

2. All source code you write for the class project is open source (particularly to me) unless you specify otherwise in your project proposal.

3. If you take on one of my research project ideas for your class project you are entitled to be credited for all of your work and contributions but you don't own the project, meaning that I reserve the right to have one of my RAs take ownership of the project in the future and possibly even leave you out.

4. If you have any concerns whatsoever about anything at any time, please come talk to me. It's very easy to make mistakes and have misunderstandings arise so please let me know if you feel like I'm not being fair. I have no problem with being generous with authorship etc. on future papers, my main concern is more that that I'll overlook a 591 student's contributions to my research agenda and unfairly exclude them and they won't say anything to me.
If you choose to work on your own research idea or something with your advisor then we don't need to worry about all of this and all decisions about authorship, attribution, etc., are between you and your advisor.