CS851: Web Applications Security Seminar

Coordinator: David Evans
Meetings: Tuesdays and Thursdays, 11am-12:15pm, Olsson 228E
Office Hours: Mondays, 10:30-11:30am; Tuesdays, 12:15-1:30pm
Website: http://www.cs.virginia.edu/evans/wass

Theme. Web applications connect people and applications in complex and dynamic ways, presenting new vectors for rapid attack and subtle channels for privacy compromise. This seminar will focus on security vulnerabilities, threats, and defenses for web applications including mashups and dynamic social networks, and "Web 2.0" technologies such as Ajax and Flash.

Topics. Relevant topics include anything related to security of web applications, broadly defined. Possible topics include (but are not limited to): anonymity, click fraud, content composition (e.g., mashups), identity and reputation services, malware, phishing, privacy, search engine poisoning, security testing, social networking vulnerabilities, static and dynamic analysis, threat modeling, vulnerability analysis.

Expected Background. The seminar is open to both graduate students and ambitious undergraduates (with permission). Students in the seminar are expected to have enough background in theory, cryptography, operating systems, security, and networks to be able to understand research papers from recent security, networking, and operating systems conferences. Students lacking relevant background will need to supplement the seminar readings with additional material.

Requirements. Each student will be expected to:
- lead a seminar meeting on one topic (with help of one or more other students)
- assist a student who is leading a seminar meeting
- write short reviews/responses to seminar papers
- complete a semester project (alone, or with a small team)

Leading and Assisting Seminar Topics. At the first meeting (Tuesday, August 28), each student will sign up to lead a seminar meeting, and to be an assistant to one other leader (depending on enrollment, some students may have an opportunity to lead two topics). The leader is expected to do most of the presentation during the seminar, but the assistant should help the leader develop the presentation. For typical topics, there will be one or two assigned papers that all students in the seminar read. The topic leaders will need to read additional papers related to the assigned papers for background and context. At least one week before the scheduled seminar, the topic leader and assistant should meet with me to discuss your plans for the presentation. You should come prepared to this meeting with a rough outline of the seminar presentation, a selection of the focus paper or papers (which all students read), a list of background and context papers, and 2-3 response questions that students will include in their reviews of the focus paper. The normal time for this meeting is Monday, 10:30am for the group going the next Tuesday; and Tuesday after seminar for the group going next Thursday. Alternative times should be scheduled as necessary.

Responses. All students taking the seminar for credit are expected to write short answers to the response questions for each focus paper. For each response, there will be three generic questions: (1) What problem does this work attempt to solve? (2) What are the most important novel contributions of the work? (3) What change or enhancement would most significantly

improve the work? In addition, there will be a few questions specific to the focus paper that will be created by the topic leaders. These questions will be posted to the course mailing list.

Projects. Students will work alone or in small teams on a research project that is broadly related to the seminar theme. By the end of the semester, each project team should produce a paper suitable for publication in a competitive conference. The deliverables for the project are:

- Tuesday, October 2 – Project Mini-Proposal. Your mini-proposal should describe the question you intend to answer, and why it is interesting.
- Thursday, October 4 and any class thereafter – "Elevator" speeches (see below).
- Tuesday, October 16 – Project Proposal (see below).
- Tuesday, December 4 or Thursday, December 6 – Project Final Presentations.
- Monday, December 10 (11:59pm) – Project Final Reports. The final reports should be conference quality papers describing your project.

Elevator Speeches. Imagine you are in an elevator with a very busy, rich and important person. You have ninety seconds (elevators in buildings with rich and important people in them tend to be faster than the one in our building) to convince her your project is so exciting she should read your proposal and consider funding it generously. In ninety seconds you should be able to explain the problem you hope to solve, why it is interesting (to someone not an expert in your area), and what you are doing to solve it. A successful elevator speech elicits a question from the listener after the elevator doors open; an unsuccessful one drives the listener away as quickly as possible. On Thursday, 4 October, each group will give an elevator speech about your project. At any class after that, students may be pseudorandomly selected to give elevator speeches about their projects. Being able to give a good elevator speech may be even more important to your future career in research or industry than being able to do good research and write well, so it is worth practicing this whenever you get the chance.

Project Proposal. The project proposal should include:

- **Clear Statement of the Problem** — what question is your project seeking to answer? If your project is successful, what will the research community know after you are done that it does not already know.
- **Motivation** — why is your problem interesting and important?
- **Related Work** — this doesn't need to be complete yet, but should be enough to show the problem is relevant and interesting and make it clear what has and has not already been solved by other researchers. You should make sure to relate the related work to your project, not just summarize a lot of papers you have read. For every work you describe, your related work section should explain clearly why it is relevant to what you want to do.
- **Research Plan** — concrete description of what you plan to do. Your research plan must include clear milestones for every week until the end of the project. If your project involves more than one person, it should also explain how you are dividing and managing the work in your team.
- **Evaluation** — description of how you will decide if the project is successful. How do you know if you have answered the problem question? Note that your project does not need to be a *successful* research project to satisfy the requirements for the course project, but you do need some way of evaluating the success of your project.

We expect most project proposals will be about 5 pages long, but there is no strict length requirement or expectation.