Updated: 15 September 2023

CSE P590B: (Special topics) Security Engineering
Paul G Allen School of Computer Science and Engineering
University of Washington
Autumn 2023
– Draft. Final Syllabus will be in Canvas –

Mondays
6:30 – 9:20 PM
Room: CSE2 G10

Instructor:

Adam Shostack
shostack@uw.edu
Office: Zoom (Link in Canvas)
Office hours: Zoom 4:30-5:30 PM Thursday

Course Assistants:

Office: Zoom
Office hours: By appointment

Office: Zoom
Office hours: By appointment

1. Course Description & Framing

Developing secure systems requires an understanding of the failure modes, and also how to build security into systems. That involves an understanding of security as a feature and security as a systems property, as well as the economic, political, and organizational factors that contribute to security being built, and market, usability, and network effects that lead to security being either part of or an obstacle to market success.

Complementing the 564 course, Security Engineering (SE) will rely on existing understanding of security flaws and how they work, and focus on the engineering techniques that students can bring to bear in delivering secure products and services. Unlike 564, which is a broad tour through computer security and which has a deep emphasis on learning from attack methodologies, SE will focus on engineering processes and techniques that produce systems that defenders can operate safely. (prevent/detect/respond) So where 564 covers memory safety by writing a buffer overflow, SE will cover selecting safer languages, and techniques for safer parsing with untrusted languages, such as sandbox architectures. The course uses a "read, discuss and explore" approach more than coding assignments, or 'configure this tool' assignments.

As an underlying principle, we will strive to be reasonable toward you, and we ask you to be reasonable toward us. These policies aim to give us some guidelines to make that happen. *If in doubt about anything, please don't hesitate to check with the course staff.*

Inclusiveness: You should expect and demand to be treated by your classmates and the course staff with respect. You belong here, and we are here to help you learn and enjoy a challenging course. Likewise, I expect you to follow the UW Student Conduct Code in your interactions with your colleagues and me in this course by respecting the many social and cultural differences among us. If any incident occurs that challenges this commitment to a supportive and inclusive environment, please let me know so the issue can be addressed.

2. Course Objectives

The course will give students an overarching view of security, and how and why to build it into products, via a mix of readings, lectures, interactive discussion and project work.

Students will be able to consider both specific appropriate defenses for a system, and engineering techniques that ensure those defenses are considered in structured, systematic and comprehensive ways.

3. Attendance and health and safety

This class is planned to be conducted in-person, and no virtual option is planned. Switching to a virtual delivery course will only be possible if the University switches all courses to that delivery method. Students are expected to participate in class to fully benefit from course activities and meet the course's learning objectives. Students should only register for this class if they are able to attend in-person. To protect their fellow students, faculty, and staff, students who feel ill or exhibit possible symptoms of transmissible disease should not come to class.

When absent, it is the responsibility of the student to inform the instructor in advance (or as close to the class period as possible in the case of an unexpected absence), and to request appropriate make-up work as per policies established in the syllabus. What make-up work is possible, or how assignments or course grading might be modified to accommodate missed work, is the prerogative of the instructor. For chronic absences, the instructor may negotiate an incomplete grade after the 8th week, or recommend the student contact their academic adviser to consider a hardship withdrawal (known as a Registrar Drop).

The pandemic is (obviously) an evolving threat to our safety, and we will follow University guidance which may change on short notice. The latest information is available at https://www.washington.edu/coronavirus/.

If mask requirements are re-introduced, they will be enforced; current guidance is that masking is ‘highly recommended’ the first two weeks of each quarter.

4. Eligibility and Prerequisites

This course is open to graduate students in the Professional Masters Program or other UW graduate students in Computer Science. Undergraduates and graduate students in other departments are encouraged to contact the professor if they believe this course would be beneficial to them, and requests will be considered on a case by case and as space allows basis. Auditors are encouraged, and will be admitted as space allows. A diversity of backgrounds enriches the course.

There are no prerequisites. Experience delivering commercial or open source software is helpful, but not mandatory.

5. Course Requirements

Students will be encouraged to participate in class discussions, and to hone their analytical skills through writing assignments.

The Allen School is a professional school, training professionals. As such, students are expected to:

(1) attend all classes;
(2) be on time;
(3) refrain from using their laptops and cell phones in class (except when useful for discussion);
(4) submit assignments on time;
(5) be respectful of each other and of the instructor;
(6) be prepared to be called upon in class at any time; and
(7) do their best to prepare professional products for their assignments.

Effective communication is a skill that professionals need. This is not a class on writing, and your writing will be evaluated for clarity. While grammar and style can contribute to effective writing, we recognize that many students did not grow up speaking or writing English, and avoid disadvantaging them.

Grades will be calculated as follows:

> Class Participation: (10%) Every student is expected to be prepared for and attend every class, and to participate in the discussions.
>
> Assignments: (55%) Students will write a set of short (500-1,000 words) assignments including a threat model analysis of a system, a re-design of that system to apply security principles, and an essay proposing improvements to an engineering system. (15% each). The essay will be peer-graded, and the responses will count for 10% of the grade. A quality rubric will be provided for each.
>
> Short Essays: (15%) Several short (250-500 word) writing assignments, some based on real-world activities, will be due throughout the semester.
>
> Final (20%): Students will propose a realistic improvement to the engineering approach to a system.

Because this is a new course, we do not have the experience to say how grades on coursework will translate to course grades. We will roughly follow Allen School PMP course norms.

6. Assignments, Grading, and Lateness

All written assignments, except for the final, will be graded according to a grading rubric which will be provided in advance. Each rubric will be in a table with points granted as columns and elements assessed as rows. For example for the threat model exercise:

	Poor (0)	Acceptable (1)	Good (2)	Excellent (3)
System model	There is no diagram	The diagram contains a person, a computer, and a lock	There is a trust boundary	Trust boundary is well placed; or diagram shows evidence of being sketched and refined

Assumptions list	None	1 -3 assumptions listed	3+ plausible assumptions listed;	Assumptions are insightful or surprising to instructors, demonstrating careful thought

The columns are “gated” — you cannot receive a “good” without first qualifying as “acceptable.”

All assignments must be uploaded to the course’s Canvas page by 9:00 AM on the date due to receive full credit. Late assignments will be marked down 1/5 of the maximum possible points for each day they are late, unless the professor grants an exception due to special circumstances.

Students will each have 3 “free late chits.” Each will excuse 24 hours of lateness. Otherwise, absences and lateness will not be excused. I understand that people are busy and overscheduled, with multiple obligations, and that occasionally something will take precedence over this class. If that is the case, I expect students to make their decision and accept the consequences. If you need an unusual exception, please reach out to the instructor.

Class participation will be graded on quality, not frequency. This is a large class, and I know that everyone can’t speak in every session. Good contributions have some of the following characteristics:

1. Clear, sound, rigorous, insightful analysis;
2. Comments that thoughtfully challenge conventional or politically safe positions;
3. Realistic recommendations for action;
4. So-called “stupid questions” that no one else is willing to ask but that open up productive paths of inquiry;
5. Constructive critique of others’ contributions; and
6. Impact on the thinking of others.

7. Readings

Students are expected to have read the required readings before class—many of the classes will be discussions of issues raised in the readings. Recommended readings represent additional resources that may be useful for students especially interested in a particular topic, but reading them is not required for class.

Readings will be a mix of book chapters, articles and essays from the popular press; and academic or legal articles. One book is assigned and is available at the University Bookstore and elsewhere.

Adam Shostack, *Threat Modeling: Designing For Security* (Wiley, 2014)

I will not profit from this assignment; I will donate the royalties to the University.

All other readings will be available on the Canvas course page.

Two other books that may be generally useful are:

1. Ross Anderson, *Security Engineering* (Wiley). The third edition (2020) is preferable. His book is an excellent reference, full of useful facts about how systems fail in the real world. https://www.cl.cam.ac.uk/~rja14/book.html
2. Paul van Oorschot, *Computer Security and the Internet* (Springer, 2020). This is a very useful compendium of both attack and defense information. Especially useful if you have not taken 484 or 564. https://people.scs.carleton.ca/~paulv/toolsjewels.html

8. Academic Integrity

Academic integrity and a solid ethical grounding are vital. They must be shown in this course.

The subject matter of this course is designed to spark discussion, and you are encouraged to talk about everything, including assignments, with your classmates. However, individual work must be done by the individual who takes credit for the work, and use of ideas imported from elsewhere must give credit to the source of the idea. This includes but is certainly not limited to the use of Large Language Models (LLMs) such as ChatGPT or Bard. Work done by an LLM must be cited and clearly distinguished from work you have done.

Clear citation is vital for building on the work of others. For example, "this syllabus is based on one by Bruce Schneier, and draws heavily on the UW CSE 564 syllabus, and details have been adjusted to reflect the plan for UW CSE 590." The form of citation is less important than clarity in what's being cited and what is your work. For example, "As Anderson discusses; In [14] the authors say X ; The principle is expressed in (van Oorschot, 2020)" are all acceptable, and should be followed with something that clearly indicates the transition to your work, such as "From that, I take…; applying that to the problem…" Good citation is a skill you should develop as part of a Masters program.

Failing to appropriately cite the work of others you've relied on is a serious violation of academic and professional integrity. Students must be familiar with and must observe University rules regarding the citation of sources. Including material from others in the assignments without appropriate quotation marks and citations is regarded, as a matter of School and University policy, as a serious violation of academic and professional standards.

9. Office Hours

Office hours are generally 4.30-5:30 PM Thursdays, or by appointment. The time is selected to be available to both those who need them to be either inside or outside work hours. I am happy to discuss the class, the assignments, your other projects, your future careers, and any other topic in cybersecurity, privacy, and related areas. Please email me for an appointment. The official syllabus in Canvas has a scheduling link as well.

The TAs are also available for office hours. Please email them for appointments.

10. Class Schedule

Note: the set of topics is subject to change, as the topic of cybersecurity and the policy debates around that topic change rapidly. Events may well dictate a different topic; if so, we will adapt. Consult the Canvas course page for the most current syllabus.

11. Detailed Syllabus, Assignments, and Reading List

The detailed reading list and assignments are maintained in Canvas.

12. Ensuring Your Needs Are Addressed

UW has a set of policies designed to ensure a respectful and inclusive learning environment. I encourage you to come to me, department staff, or the resources listed below.

Washington state law requires that UW develop a policy for accommodation of student absences or significant hardship due to reasons of faith or conscience, or for organized religious activities. The UW's policy, including more information about how to request an accommodation, is available at Religious Accommodations Policy (https://registrar.washington.edu/staffandfaculty/religious-accommodations-policy/). Accommodations must be requested within the first two weeks of this course using the Religious Accommodations Request form (https://registrar.washington.edu/students/religious-accommodations-request/).

Embedded in the core values of the University of Washington is a commitment to ensuring access to a quality higher education experience for a diverse student population. Disability Resources for Students (DRS) recognizes disability as an aspect of diversity that is integral to society and to our campus community. DRS serves as a partner in fostering an inclusive and equitable environment for all University of Washington students. The DRS office is in 011 Mary Gates Hall. Please see the UW resources at http://depts.washington.edu/uwdrs/current-students/accommodations/

UW, through numerous policies, prohibits sex- and gender-based violence and harassment, and we expect students, faculty, and staff to act professionally and respectfully in all work, learning, and research environments.

For support, resources, and reporting options related to sex- and gender-based violence or harassment, visit UW Title IX's webpage, specifically the Know Your Rights & Resources guide.

Please know that if you choose to disclose information to me about sex- or gender-based violence or harassment, I will connect you (or the person who experienced the conduct) with resources and individuals who can best provide support and options. You can also access those resources directly:

- Confidential: Confidential advocates will not share information with others unless given express permission by the person who has experienced the harm or when required by law.
- Private and/or anonymous: SafeCampus provides consultation and support and can connect you with additional resources if you want them.You can contact SafeCampus anonymously or share limited information when you call.

Please note that some senior leaders and other specified employees have been identified as "Officials Required to Report." If an Official Required to Report learns of possible sex- or gender-based violence or harassment, they are required to call SafeCampus and report all the details they have in order to ensure that the person who experienced harm is offered support and reporting options.

Title IX website: uw.edu/titleix/

Survivor resources page: uw.edu/titleix/survivor-resources/

Confidential advocates: uw.edu/sexualassault/support/advocacy/

SafeCampus: uw.edu/safecampus/

Officials Required to Report: uw.edu/titleix/employee-reporting-expectations/

Related policies: uw.edu/titleix/policies/