SFWE 401/501: Software Assurance and Security
Course Syllabus

Instructor: Dr. Pratik Satam
Contact Information: pratiksatam@arizona.edu
Phone: 520-626-072
Office: ENGR 268

Course Description

Software plays a vital role in modern life, managing essential services, like the financial systems, social networks, the Internet, and Cyber-Physical Systems, to name a few. Modern software must be bug-free, secure, and function reliably while controlling our critical systems. Software Assurance is the level of confidence in software being free of intentional or accidental vulnerabilities (including flaws, faults, and bugs) inserted at any time during its lifecycle.

Through this course, the students will learn critical concepts in Software Assurance and Security, ensuring a complete understanding of processes, procedures, and tools required to design, build, and sustain secure software. This course will cover the following topics:

- Secure Software Development Life Cycle
- Software Vulnerability analysis
- Software Vulnerability frameworks
- Secure Software Development Techniques
- Coordinated Vulnerability Disclosure
- Frameworks to analyze the Software Assurance Maturity Models
- Regulations on Software Assurance.

This course will evaluate the student's performance with homework, labs, knowledge checks, midterm exams, semester projects, and a comprehensive final exam. The labs, offered through the Cybersecurity Lab as a Service (CLaaS) environment, enable the students to learn hands-on the Software Assurance Concepts learned in class. The semester project will require the students to work

in teams of three or four to evaluate and improve software assurance using industry best practices and software assurance tools.

Course Objectives:

During this course:

1. The students will be introduced to Software Assurance and Secure Software Development Life Cycle, emphasizing the importance of security in a Software Development Life Cycle. The students will use the Secure Software Development Life Cycle (SDLC) in their class project to improve the security of a vulnerable software.
2. Threat modeling plays a critical role in understanding the strengths and vulnerabilities of a system. The students will learn threat modeling and its application to software.
3. Software can have different types of vulnerabilities, faults, and bugs. In this course, the students will learn about these vulnerabilities through Common Weakness Enumeration (CWE) Frameworks and the Bugs Framework (BF). The labs will provide a deeper understanding of these vulnerabilities by allowing students to perform the studied attacks on vulnerable software. The students will use these frameworks in their class project to understand, identify, and implement vulnerabilities.
4. Static code analysis tools are used to identify software vulnerabilities, flaws, and bugs during the Software Development Life Cycle. The students will learn the concepts of Static Application Security Testing (SAST). The labs will allow them to use SAST tools on vulnerable software, enforcing the concepts learned in the class. The students will use this complete understanding of the SAST in their class project to improve the Software Assurance of vulnerable software.
5. Through the in-class instruction and the labs, the students will learn defensive coding practices and the concept of the principle of least privilege.
6. In a Software Development Life Cycle (SDLC), a team will find bugs and vulnerabilities in their deployed software. It is critical to have a process to address these findings with software patches through the software development process. The students will be introduced to the Coordinated Vulnerability Disclosure process to evaluate bugs, develop patches, and inform the users.
7. The students will learn about the Open Web Application Security Project (OWASP) Software Assurance Maturity Model, a framework to measure the performance of the Secure Software Development Life Cycle.
8. Through this course, students will learn about software security and assurance regulations.

Expected Learning Outcomes:

Upon the completion of this course, students should be able to:

1. Develop a secure software development cycle capable of assuring the security of the software they have produced. [ABET Student Outcome 1, ABET Student Outcome 2, ABET Student Outcome 7].
2. Develop secure software for managing essential modern services while ensuring the software is bug, fault, and vulnerability free. [ABET Student Outcome 4].

3. Evaluate and measure the security of a software system by identifying (and documenting) the bugs, reporting them to the community, and developing patches to fix them. [ABET Student Outcome 1, ABET Student Outcome 2, ABET Student Outcome 3, ABET Student Outcome 4, ABET Student Outcome 6, and ABET Student Outcome 7].
4. Conduct a software design review while being part of a team of subject matter experts. [ABET Student Outcome 3, ABET Student Outcome 5, ABET Student Outcome 6].
5. Conduct a review of the software development processes of an organization while being part of a team of subject matter experts. [ABET Student Outcome 3, ABET Student Outcome 5, ABET Student Outcome 6].
6. Develop software compliant with global regulations. [ABET Student Outcome 2, ABET Student Outcome 4].
7. Graduate students only: Design and develop secure software free of vulnerabilities and assure their performance through SAST.

Course Prerequisites:

The prerequisites for this course are: ECE 275

Course Format and Teaching Methods:

This course is structured around weekly progress. It will include a combination of lectures, online labs, and small groups activities focused on experiential learning, in-class discussions, and individual assessments. The expected weekly progress is outlined in the course schedule. At a minimum it is recommended that students keep up with coursework by following the outlined course schedule on D2L. Note the **DUE DATES** on course deliverables are all posted on D2L.

This course is architected to engage and demonstrate key concepts of the materials covered using collaborative and active learning strategies. Students will watch pre-recorded lecture materials that have interactive features integrated into the materials. Interactive instructional technologies (Cybersecurity Lab as a Service (CLaaS), PlayPosit, Perusall, etc.) and industry-relevant software development tools will be used to allow students to demonstrate and self-assess their progress toward and achievement of course learning outcomes. Students will break into small teams to work on activities that demonstrate the key principles covered in the lectures.

Course Communications:

Announcements and important reminders will be regularly posted on D2L. Log in frequently to check for new announcements, reminders, and information related to the course.

Students are encouraged to reach out to the instructor frequently throughout the semester via in-person lectures, email, phone call, text, office hours, or schedule an in-person or Zoom meeting. Every

attempt will be made to respond to any questions or concerns that you may have within 24 hours, if possible (often sooner).

Textbooks:

The textbook recommended for reading in this course:

- Software Security: Building Security in- 1st Edition
  Authors: Gary McGraw
  ISBN-13: 978-0321356703
  ISBN-10: 9780321356703

Other Supplemental Readings / References:

Although the textbook is a recommendation, we consider the following free online sources as our main sources of reading:

- NIST Secure Software Development Framework (SP 800-218)
- NIST Data Centric Threat Modeling (SP 800-154)
- The Common Weakness Enumeration (CWE)
- Bug Framework
- The MITRE ATT&CK Framework
- OWASP Software Assurance Maturity Model (Barebones Model)

Additional supplemental materials will be referenced and provided to students via D2L.

Course Schedule

The following table provides an outline for the topics and objectives that will be covered during each module for this course. Specific dates will be posted on D2L for any given semester.

Module	Topic	Learning Outcomes
1	Introduction to Software Assurance and Security	• Introduce the security problems with software. • Provide use cases of vulnerable software and associated losses. • Introduce software assurance.
2	Secure Software Development Life Cycle	• Explain the importance of security in the SDLC. • Explain different secure SDLC architectures.
3	Threat Modeling for Software	• Explain threat modeling for software. • Describe threat modeling use cases. • Explain STRIDE and DREAD models for threat modeling. • Explain OCTAVE model for threat modeling
4	Software Vulnerabilities: Common Weakness Enumeration (CWE) and Bugs Framework (BF)	• Introduce the CWE and BF vulnerability framework. • Explain the 6 categories of software vulnerabilities with example.
5	Defensive Coding practices, permission, and principle of least privilege	• Explain and demonstrate Defensive Coding Practices. • Explain the principle of least privilege and permission in software systems.
6	Static Application Security Testing (SAST)	• Introduce static code analysis techniques. • Describe testcases for software vulnerability analysis. • Introduce tools for static analysis of software • Evaluate software security and vulnerabilities using different static analysis tools.
7	Coordinated Vulnerability Disclosure	• Introduce the Coordinated Vulnerability Disclosure process. • Describe the steps in the Coordinated Vulnerability Disclosure Process: 1) Collection, 2) Analysis, 3) Mitigation Coordination, 4) Application of Mitigation, 5) Disclosure. • Describe the integration of the Coordinated Vulnerability Disclosure process into the SDLC.

Module	Topic	Learning Outcomes
8	OWASP Software Assurance Maturity Model	• Introduce the OWASP Software Assurance Maturity Model. • Describe the four functions in the Software Assurance Maturity Model, and explain the practices to access the maturity of the software development lifecycle. • Demonstrate the application of the Software Assurance Maturity Model to different use cases.
9	Regulations on Software Assurance and Security	• Introduce the regulations for software • Explain the impact of regulations: 1) HIPAA, 2) FERPA, and 3) GDPR. • Study the impact of these regulations on software with case studies

D2L Course Management System

This course uses the University of Arizona's D2L course management system. You are **required** to use D2L with this class and are encouraged to check our D2L class course space daily.

You are also encouraged to have D2L email forwarded to your primary University of Arizona email account. We will use D2L for course assignments, exams, content distribution, and important announcements. The University of Arizona's D2L system is available at: http://D2L.arizona.edu.

Course Assignments and Exams

There will be homework assignments aligned to the outcomes of the module and designed to assess students' progress toward the course outcomes. There will be lab assignments aimed at providing students deeper, practical understanding to the material covered in-class. There will also be graded module-based discussion board prompts; student participation is required. There will be one midterm exam and a final exam. All exams will be timed, administered by the instructor or proctor, and will be available during the regularly scheduled exam time. ***Note: the instructor will give students ample notice of the format, time, and any resulting stipulations about where and how the exams will be administered.***

Final Examination:

The date and time of the final exam or project, along with links to the Final Exam Regulations can be found at https://www.registrar.arizona.edu/courses/final-examination-regulations-and-information, and Final Exam Schedule, http://www.registrar.arizona.edu/schedules/finals.htm

Grade Distribution

The grading distribution for course assignments, class participation, semester project, and exams is as follows:

Homework Assignments (x4):	10%
Note: *Graduate students will be required to answer extra questions focused on design and development aspects of the topics*	
Lab Assignments (x4):	10%
Note: *Graduate students will be required to perform add-on tasks and answer extra questions requiring application and analysis of the concepts*	
Class Participation (x8):	10%
Knowledge Checks:	10%
Midterm Exam (x1):	15%
Semester Project:	25%
Comprehensive Final Exam:	20%
Note: *Graduate students will have a more comprehensive set of deliverables focusing on design and development of secure software*	
Total	**100%**

Rubrics will be posted on D2L for all homework assignments.

Grading Scale and Policies:

The following scale will be used to award the final grades:

Percentage	Letter Grade
90% – 100%	A
80% – 89%	B
70% – 79%	C
60% – 69%	D
<60%	E

Homework and labs are due at the time specified in the course schedule and/or D2L content pages. Late homework, labs, and projects will not be accepted without prior approval by the instructor and will receive 0 points.

Subject to change:

The contents of this syllabus are subject to change at the instructor's discretion.

Course Time Zone:

All dates and times mentioned in this course represent Mountain Standard Time (Arizona), which is UTC-7 hours. Arizona does not observe Daylight Savings Time. You can use the following link to get the current local time in Tucson, Arizona: http://www.timeanddate.com/worldclock/city.html?n=393

Academic Policies and Institutional Resources

Academic Policies and Procedures:

As a University of Arizona student, you are expected to become familiar with and abide by the university-wide policies and procedures. You can find complete, up-to-date information at: https://academicaffairs.arizona.edu/syllabus-policies.

Course Policies

Make-up exams:

A make-up exam may only be given under extraordinary circumstances. The student requesting a make-up exam should contact the instructor well in advance and provide *written* documentation for the reason that he/she will not be able to attend the regularly scheduled exam. It is up to the discretion of the instructor to accept the justification provided by the student.

Requests for incompletes (I) and withdrawal (W) must be made in accordance with University policies which are available at http://catalog.arizona.edu/2015-16/policies/grade.htm#I and

http://catalog.arizona.edu/2015-16/policies/grade.htm#W respectively.

Dispute of Grade Policy:

You can dispute any grade that you receive within two weeks that the grade has been awarded.

Incomplete (I) or Withdrawal (W):

Requests for incomplete (I) or withdrawal (W) must be made in accordance with University policies, which are available at http://catalog.arizona.edu/policy/grades-and-grading-system#incomplete and http://catalog.arizona.edu/policy/grades-and-grading-system#Withdrawal respectively.

Classroom Behavior Policy:

To foster a positive learning environment, students and the instructor have a shared responsibility. We want a safe, welcoming, and inclusive environment where all of us feel comfortable with each other and where we can challenge ourselves to succeed. To that end, our focus is on the tasks at hand and not on extraneous activities (e.g., texting, chatting, reading a newspaper, making phone calls, web surfing, etc.).

Online Collaboration/Netiquette:

In this course, you will primarily communicate with the instructor and peers through a variety of tools such as discussion forums, Jamboard, email, and other forms of web conferencing. The following guidelines will enable everyone in the course to participate and collaborate in a productive, safe environment.

- Be professional, courteous, and respectful as you would in a physical classroom.
- Online communication lacks the nonverbal cues that provide much of the meaning and nuances in face- to-face conversations. Choose your words carefully, phrase your sentences clearly, and stay on topic.
- It is expected that students may disagree with the research presented or the opinions of their fellow classmates. To disagree is fine but to disparage others' views is unacceptable. All comments should be kept civil and thoughtful. Remember that this course abides by university policies regarding disruptive behavior: http://policy.arizona.edu/education-and-student-affairs/disruptive-behavior-instructional-setting
- Compose your messages and posts in a word processing tool and check your spelling and grammar before submitting your post / email.

Statement of copyrighted materials:

All lecture notes, lectures, study guides and other course materials disseminated by the instructor to the students, whether in class or online, are original materials and reflect intellectual property of the instructor or author of those works (with the exception of other published reference materials – i.e. course textbooks). All readings, study guides, lecture notes and handouts are intended for individual use by students. You may not distribute or reproduce these materials for commercial purposes without the express written consent of the instructor. Students who sell or distribute these materials for any use other than their own are in violation of the University's Intellectual Property Policy (available at http://ogc.arizona.edu/node/16). Violations of the instructor's copyright may result in course sanctions and violate the Code of Academic Integrity.

Student Support:

The instructor is available to assist with **content-related** issues. You may, at any time, email the instructor. This course also provides an ***Ask the Instructor*** discussion forum within the D2L environment. You are encouraged to post content-related questions to this forum at any time, especially for things that will benefit all students. *(It is not recommended that you use this forum for individual questions that are specific to your work or performance in the class.)* This forum will be monitored on a regular basis and the instructor will respond in a timely fashion. It is common for other students to participate in answering questions posted in the ***Ask the Instructor*** forum. You should feel free to contribute to the solution if you can provide knowledge or guidance related to the question.

The following are guidelines for requesting support:

- **General Course Questions:** Use the ***Ask the Instructor*** discussion forum for questions regarding course materials or policy.
- **Personal Course Questions**: Email the instructor to discuss grades or personal concern.
- **D2L Support Questions**: Email mailto:d2l@arizona.edu

Accommodations for Students with Disabilities:

At the University of Arizona, we strive to make learning experiences as accessible as possible. If you anticipate or experience barriers based on disability or pregnancy, please contact the Disability Resource Center (520-621-3268, https://drc.arizona.edu/)to establish reasonable accommodations.

See http://drc.arizona.edu/instructors/syllabus-statement.

Library Support:

The University of Arizona Libraries provides the research tools you need at any time. For an abbreviated list of resources directly related to a specific course, select the **Library Tools** link (located in the Tools drop down on the left of the screen within the Course Navigation bar).

Course Grievance Policy:

In case of grievances with a course component or grading, students are encouraged to first try and resolve the issue with the instructors. If you feel the issue is not resolved satisfactorily, please send an email to https://registrar.arizona.edu/faculty-staff-resources/grading/grading-policies/grade-appeal.

Course Surveys and Evaluations:

Near the end of each semester / session, students will receive an invitation via email to complete an online course survey associated with this course administered by the Office of Instruction and Assessment thru the UA Student Course Survey (SCS) tool. Refer to the Student Support website associated with the Student Course Surveys (https://scs.arizona.edu/content/5).

Your feedback is extremely valuable and will be used to make changes and enhancements to the course to better meet student needs in the future.

Additional Resources for Students (recommended links):

- Student Assistance and Advocacy information is available at: http://deanofstudents.arizona.edu/student-assistance/students/student-assistance
- Confidentiality of Student Records: http://www.registrar.arizona.edu/ferpa/default.htm