SER335: Engineering Secure Software Systems **Fall 2021 Session B (online)**

Course Description:

Software Engineering principles applied to securing software systems. Software lifecycle processes contextualized to security needs of software. Software requirements analysis and software verification and validation practices for security. Software architecture security assessment. Software engineering organization policies for security, including threat modeling and assessment, vulnerability classification, risk management, and preparing for security audits.

Prerequisites:

- SER216, SER315 (co-requisite), SER334 (co-requisite)
- A desire to learn and participate in class.

Required Information:

1. Contact Information

(Instructor) Kevin Gary, Peralta 230C, Ph. 7-1373
Email: kgary@email.asu.edu
Zoom: ASU Zoom https://asu.zoom.us/j/7355426020

2. Office Hours

Office hours will be conducted via Zoom from 9:30am-11am MW and M 4-5 or by appointment.

Teaching Assistant (Shubhangi Gupta, sgupt239@asu.edu) will have office hours posted at the start of the session on Canvas

3. Course Objectives and Expected Learning Outcomes

CO1. (PO-3) Describe key concepts in security fundamentals
CO2. (PO-SER2) Analyze completeness and correctness of security requirements for a software system
CO3. (PO-6, PO-SER2) Apply appropriate verification and validation techniques to software
CO4. (PO-3, PO-SER1) Construct a risk management plan for software architecture vulnerabilities
CO5. (PO-1, PO-SER2) Model underlying program construction, build, deployment, and execution to identify software vulnerabilities
CO6. (PO-4) Explain the importance of software security in modern life from ethical and societal impact perspectives.

4. Grading Policies

20% 1 final exam
15% Case study
15% Quizzes (7 will be given, top 5 used @ 3% each)
50% Labs (6 labs given, drop the lowest lab grade)

Grade Appeals:
Students have the right to appeal a grade in writing. Submit your appeal **via email (no Slack) to** kgary@email.asu.edu with the graded **assignment**, stating the reason for your appeal. All appeals must be turned in no later than one week after the **graded** material has been returned to you. For the last lab, you will only have one day to appeal due to the end of the semester. Grade appeals or queries are ***never*** sent to anyone other than Dr. Gary (failure to follow this policy forfeits the right to appeal).

5. ASU Attendance & Make-Up Policies

Quizzes, labs, and the case study assessment under are not excused, nor is an absence from the exams Students unable to keep up with class, take quizzes/exams, or complete lab assignments due to a medical condition must present a doctor's signed excuse and notify the instructor as soon as the condition affects the student's work. Accommodations will be made for religious observances provided that students notify the instructor at the beginning of the semester concerning those dates. Students who expect to miss class due to officially university-sanctioned activities (including military service) should inform the instructor early in the semester as soon as they are aware of the activity. Alternative arrangements will generally be made for any examinations and other graded in-class work affected by such absences.
[Note: The preceding policies are based on ACD 304–04, "Accommodation for Religious Practices" and ACD 304–02, "Missed Classes Due to University-Sanctioned Activities."]

6. Readings, Assignments, Examinations, Special Materials, Required Activities

- **Required Text**: Ian Sommerville, *Software Engineering (10th ed)*, ISBN-10: 0-13-394303-8, ISBN-13: 978-0-13-394303-0, Pearson Education, 2016.
- **Recommended Texts**:
  - *Introduction to Computer Security*, Michael T. Goodrich and Roberto Tamassia, Addison Wesley 2011 (new edition due out February 2021)
  - *Secure Software Development (4th ed. 2018)*, Jason Grembi, Cengage Publishing
- **Other readings as assigned by the instructor**.

7. Classroom Behavior / Netiquette

I take netiquette seriously. ASU's netiquettepolicy governing acceptable conduct in online settings is listed on Canvas and available at https://asuonline.asu.edu/newsroom/online-learning-tips/netiquette-online-students. Please refrain from profane language, negative or degrading comments towards peers and teaching staff, and any form of cyberbullying on Slack, email, discussion forums, and all forms of electronic communication. I consider this policy in effect even on student run discussion forums such as discord, as you are bound by ASU's and the Fulton Schools' Codes of Conduct. Any violent or threatening conduct by an ASU student in this class will be reported to the ASU Police Department and the Office of the Dean of Students. I will also report students to the Dean of Students in the event of disrespectful behavior towards the teaching staff of this course.

8. Academic Integrity

All students in this class are subject to ASU's Academic Integrity Policy (available at http://provost.asu.edu/academicintegrity) and should acquaint themselves with its content and requirements, including a strict prohibition against plagiarism. All violations will be reported to the Dean's office, who maintain records of all offenses. Students are expected to abide by the FSE Honor Code (http://engineering.asu.edu/integrity/).

The Student Academic Integrity Policy of Arizona State University requires each student to act with honesty and integrity and to respect the rights of others in carrying out all academic assignments. There are a number of actions that constitute a violation of the policy. These actions in this course include, but are not limited to:

1) practicing any form of academic deceit;
2) referring to materials or sources or employing devices (e.g., audio recorders, crib sheets, calculators, solution manuals, or commercial research services) not specifically authorized by the instructor for use during tests, quizzes, homework, and class activities;
3) acting as a substitute for another person in any academic evaluation or using a substitute in any academic evaluation;
4) possessing, buying, selling, or otherwise obtaining or using, without appropriate authorization, a copy of any materials intended to be used for academic evaluation in advance of its administration;
5) depending on the aid of others to the extent that the work is not representative of the student's abilities, knowing or having good reason to believe that this aid is not authorized by the instructor;
6) providing inappropriate aid to another person, knowing or having good reason to believe the aid is not authorized by the instructor;
7) submitting the ideas or work of another person or persons without customary and proper acknowledgment of sources (i.e., engaging in plagiarism);
8) permitting one's own ideas or work to be submitted by another person without the instructor's authorization; or attempting to influence or change any academic evaluation or record for reasons having no relevance to class achievement.
9) turning in work/code done by someone else or another pair/group
10) copying work/code done by someone else or another pair/group
11) writing code together with someone else or with another pair/group (unless expressly allowed by the instructor)

A common question in technical courses is the use of code or other work that is "googled" or found on popular sites such as StackOverflow. Items 5 and 7 pertain to this situation. Most programmers use reference examples, found in print or online. This is fine as a practice but is not acceptable in situations where you are using code to proxy *your understanding of the technical concepts* applied in that assessment (i.e. lab). First, if you are uncertain if it is allowable or not, verify directly with the instructor before submitting the assignment. Second, if it is allowable, you are still required to a) adhere to all originating author's constraints on the use and licensing of the artifact, and b) provide proper attribution (full URL to the code snippet or bibliographic reference to a print item). Failure to do so constitutes a violation of this Academic Integrity Policy.

The penalty for an Academic Integrity Violation (cheating) on a quiz will be a reduction of one full level of your course letter grade for the first offense, and failure of the course for a second offense. The penalty for an Academic Integrity Violation (cheating) on an exam or lab is immediate failure of the course. The penalty for a plagiarism violation on the case study will be a penalty of at least 1/3 of the case study grade, potentially up to a zero grade based on cardinality and severity. All violations will be referred to the Dean's Office of the Ira A. Fulton Schools of Engineering.

9. Disability Accommodations.

Suitable accommodations will be made for students having disabilities and students should notify the instructor as early as possible if they will require same. Such students must be registered with the Disability Resource Center and provide documentation to that effect.

10. Sexual Discrimination

Title IX is a federal law that provides that no person be excluded on the basis of sex from participation in, be denied benefits of, or be subjected to discrimination under any education program or activity. Both Title IX and university policy make clear that sexual violence and harassment based on sex is prohibited. An individual who believes they have been subjected to sexual violence or harassed on the basis of sex can seek support, including counseling and academic support, from the university. If you or someone you know has been harassed on the basis of sex or sexually assaulted, you can find information and resources at https://sexualviolenceprevention.asu.edu/faqs. As a mandated reporter, I am obligated to report any information I become aware of regarding alleged acts of sexual discrimination, including sexual violence and dating violence. ASU Counseling Services, https://eoss.asu.edu/counseling, is available if you wish to discuss any concerns confidentially and privately.

11. Other Notices:

Notice: Any information in this syllabus may be subject to change with reasonable advance notice.

Notice: All contents of lectures, including written materials distributed to the class, are under copyright protection. Notes based on these materials may not be sold or commercialized without the express permission of the instructor. [Based on ACD 304-06.]

Additional Course Information:

This course covers Software Security from a Software Development Lifecycle (SDLC) perspective. Course topics are presented as *modules* that you will see on Canvas. Modules 0 and 1 are required in week 1, thereafter one module per week.

Module 0: Computer Networking Overview (may be review for some)
Module 1: Overview of Computer Security
Module 2: Information Technology Security - Physical, Host, and Basic Network security
Module 3: Security in the SDLC, Software Security Requirements, and Security Standards
Module 4: Verification & Validation (V & V) for Security - Penetration testing, Experience testing, Static analysis
Module 5: Security and Software Construction
Module 6: Security and Software Architecture and Design
Module 7: Social Impacts of Security and Risk Management Frameworks

Assessments:

Quizzes (15%):

- There will be one quiz per week in the week when the module is covered. These are due every Tuesday evening by 11:59pm.
- Make-ups will not be given for missed quizzes (except for excused absences described above), though note I will take the top 5 scores for this portion of your grade (3% each) so if you miss one you may drop it.

Final Exam (20%):

- As required by ASU's Academic Calendar, the final exam will be open on Friday December 3rd (the last day of the session), and I will leave it open until 5pm Arizona time Saturday December 4 to accommodate the online students who work during the week.
- You will be required to use ASU's proctoring solution, HonorLock, while taking the exam. You must follow all instructions for your environment, such as having a functioning webcam, no headphones or other devices present, and a single-monitor setup.

Case Study (15%):

You will be assigned a written analysis of a case study early in the session. You will complete this case study with a partner.

Lab assignments (50%):

- There will be 6 traditional programming/technology labs. The labs will be intensive and students are expected to start lab assignments early to achieve successful results.
- Each lab will be worth 10 % of your grade, with the lowest lab grade being dropped.
- Time-on-task will vary by personal skillset but anticipate spending 8-15 hours on labs.
- Labs are usually due on the Monday after the Module completion date (The last lab I give you an extra day due to Thanksgiving)

Communication Policy:

- This course will use Slack as the primary communication tool outside class. I will check Slack each morning and each evening Monday-Friday. Your teaching staff will also check on Slack each day at times that work with their personal schedules. I will try to check Slack and email on Saturdays but this is variable due to my personal constraints. I am strictly not available on Sundays.
- When you have a question, please ask it in an appropriate channel. Please do not use Direct Messages (DMs) unless it is a personally sensitive matter (and even then, you should probably use email).
- Email is the only allowed medium for a grade appeal, and only to me (Dr. Gary) at kgary@email.asu.edu.
- I know ASU's email system will try and get you to email me at kgary@asu.edu, but try to remember to use kgary@email.asu.edu. I reserve this email for student class traffic, and therefore can be more responsive (I will check this twice per day also).
- Do not interpret communication on Slack as a change in lab requirements. If a question on lab requirements comes up during class and I need to clarify or modify something, a Canvas announcement will be posted.
- Please take the netiquette policy (stated above) seriously. I like to have a warm communal academic environment, and Slack is the closest thing we will come to a classroom experience, so let's keep it a 100% positive community.
- Office hours will be conducted on Zoom. You may be asked to sit in the waiting room if I am meeting with a student who joined ahead of you. You are required to have a webcam on if you connect.

Late policies:

- Late submissions are not allowed unless a prior exemption has been given by the instructor. Religious observances and documented medical and family emergencies are accommodated as stated above.
- I am aware that this academic year, like the last, is being conducted under unusual circumstances and may cause a higher level of stress than a typical year. Please communicate with me to find a successful pathway through these times.