SIE 573: Engineering of Trustworthy Secure Systems

Course Syllabus

Primary Instructor: Bill Hayes

Email: billhayes@email.arizona.edu

847-404-0136

Office Hours: *TBR via Zoom*

***Guest Instructor*:** Sharon ONeal

sharononeal@email.arizona.edu

520-822-4040

Course Description

The purpose of this course is to explore widely accepted security frameworks, industry standards, and techniques employed in engineering trustworthy secure and resilient systems. We will study and explore several National Institute of Standard and Technology (NIST) frameworks such as the Cyber Security Framework (CSF), the Risk Management Framework (RMF), and other standards. These widely adopted standards have been developed to ensure that the appropriate security principles, concepts, methods, and practices are applied during the system development life cycle (SDLC) to achieve stakeholder objectives for the protection of assets—across all forms of adversity characterized as disruptions, hazards, and threats. We will also explore case studies within the Department of Homeland Security's (DHS) 16 Critical Infrastructure elements (shown in the figure below), to understand how government and private sector participants within the critical infrastructure community work together to manage risks and achieve security and resilient outcomes. Cyber resiliency is the ability to anticipate,

withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources regardless of the source.

Upon completion of the course, students will gain experience in understanding, assessing and complying with the various NIST and DHS frameworks and standards in order to proactively design security features into systems/products to prevent or minimize asset loss or compromise, and reduce system defects that can lead to security vulnerabilities that could render a system susceptible to exploitation. They will also learn how to develop systems that are more cyber resilient.

Course Objectives:

Upon completion of this course, students will be able to address the major questions, challenges, and processes that Systems Security Engineers (SSE) face in evaluating the cyber risk and resiliency associated with a large-scale system. A diverse and varied set of topics will be covered to give students a fundamental understanding of the Cyber Security landscape, and will include the following:

1. Cyber Security Framework
2. Risk Management Framework
3. Systems Security Engineering Framework
4. Cyber Resiliency Engineering Framework
5. Common Vulnerabilities and Exposures (CVEs)
6. Foundations, principles, methods, and tools for developing more cyber resilient designs
7. Understanding how and where cyber resiliency factors should be considered throughout the SDLC
8. Becoming familiar with cyber resiliency techniques, design principles, and implementation approaches

Expected Learning Outcomes:

Students will be able to address the major questions and issues that System Security engineers face including:

- How does an SSE use the CSF to guide the development of a cyber resilient system?

- How does an SSE use the RMF to categorize, select, implement, assess, monitor and authorize controls used to minimize the cyber risk in a system?
- What are fundamental aspects of a cyber resilient system?
- Which cyber resiliency objectives are most important to a given stakeholder?
- To what degree can cyber resiliency objectives be achieved?
- How quickly and cost effectively can cyber resiliency objectives be achieved?
- With what degree of confidence or trust can each cyber resiliency objective be achieved?

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

1) Identify, formulate, and solve complex engineering problems in Systems Security Engineering and Cyber Resiliency by applying multifaceted principles of engineering, science, and mathematics. [ABET Student Outcome 1]

2) Communicate effectively, through both written technical reports, team projects, and oral presentations related to cyber resiliency within the 16 Critical Infrastructures as defined by the DHS. [ABET Student Outcome 3]

3) Recognize and address both ethical and professional responsibilities in cyber policy, standards and engineering, resulting in informed decisions and approaches that impact cyber research and solutions in global, economic, environmental, and societal contexts. [ABET Student Outcome 4]

4) Work cooperatively as a multidisciplinary team, whose team members work together to provide leadership, create a collaborative and inclusive environment, establish goals, plan tasks, and meet objectives in solving Cyber related problems/research/evaluations. [ABET Student Outcome 5]

5) Demonstrate the ability to develop and apply cyber related engineering design considerations to produce solutions that incorporate public health, safety, security and welfare, as well as global, cultural, social, environmental, and economic factors. [ABET Student Outcome 6]

6) Conduct a security /compliance assessment of a system within one of the 16 Critical Infrastructure sectors using the NIST Frameworks / documents as required standards. [Team project – ABET Student Outcome 7]

7) Develop detailed written guidelines to accompany the security / compliance assessment noted in item 6 above, with the goal of identifying specific security controls for any shortcomings that may be uncovered during a security/compliance assessment as it relates to a specific critical infrastructure sector. This requires the additional reading and analysis of the NIST Special Publication 800-53, “Security and Privacy Controls for Federal Information Systems and Organizations”. This is an extension of the ABET Student Outcomes 1, 3 and 6.

Course Prerequisites: A basic course in computing or computer applications (ECE 175, CSC127A, or equivalent) or consent of the instructor. Learners (including pre-med students and undergraduate biomedical, computer, electrical, systems engineering, and computer science students), trainees, fellows (including clinicians), graduate

students, and scientists from all fields with interest in either biomedical and healthcare applications or computing are welcome.

NOTE: SIE 471 / 571 is recommended, but not a firm pre-requisite for enrollment in this course.

Course Format and Teaching Methods:

This course is structured around weekly progress. It will include a combination of lectures, and small groups projects focused on experiential learning, in-class discussions, and web-based 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.

Course Communications:

Please reach out to your instructors via email, phone call, text, or schedule an in-person meeting if geographically convenient to the student. We will make every attempt to respond to any questions or concerns that you may have within 24 hours if possible.

Class Attendance / Participation Policy:

The UA's policy concerning Class Attendance, Participation, and Administrative Drops is available at: http://catalog.arizona.edu/policy/class-attendance-participation-and-administrative-drop

Participating in this course is vital to the learning process. As such, timely participation in online discussions and/or any team projects is absolutely required. Students are expected to access the course twice a week. At a minimum it is recommended that students keep up with coursework by following the outlined course schedule and notifications that will be posted on D2L. Note **DUE DATES** on course deliverables will be documented both on the course calendar located on D2L and in the Content section of D2L.

Absences may affect a student's final course grade. If you anticipate being absent, are unexpectedly absent, or are unable to participate in class online activities, please contact the instructors as soon as possible. To request a disability-related accommodation to this attendance policy, please contact the Disability Resource Center at (520) 621-3268 or drc-info@email.arizona.edu. If you are experiencing unexpected barriers to your success in your courses, the Dean of Students Office is a central support resource for all students and may be helpful. The Dean of Students Office is located in the Robert L. Nugent Building, room 100, or call 520-621-7057.Students who miss deadlines

The UA policy regarding absences for any sincerely held religious belief, observance or practice will be accommodated where reasonable, http://policy.arizona.edu/human-resources/religious-accommodation-policy.

Absences pre-approved by the UA Dean of Students (or Dean Designee) will be honored. See: https://deanofstudents.arizona.edu/absences

Textbooks:
There are no specific textbooks used for this class. However, there are numerous standards published by the National Institute of Technology (NIST) that will be heavily referenced and used, including:

- National Institute of Standards and Technology, Security and Privacy Controls for Information Systems and Organizations, Special Publication 800-53.
- National Institute of Standards and Technology, Risk Management Framework for Information Systems and Organizations – A System Life Cycle Approach for Security and Privacy, Special Publication 800-37.
- National Institute of Standards and Technology, Systems Security Engineering – Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems - Volume 1, Special Publication 800-160 Volume 1.
- National Institute of Standards and Technology, Developing Cyber-Resilient Systems, A Systems Security Engineering Approach, Volume 2, Special Publication 800-160 Volume 2.

Other Supplemental Readings / References: *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	Objective
1	**Making the Case: Factoring in Security Throughout the System Development Life Cycle (SDLC)**	• Learn why following and complying with Cyber focused industry standards is critical to system development • Understand the need for Cyber resiliency
2	**Understanding System Security Engineering**	• Explore the System Security Engineering Framework • Explore SSE activities and tasks • Explore SSE Outcomes • Explore the CVE database and categorization
3	**Case Study: A Supervisory Control and Data Acquisition (SCADA) System Overview**	• Learn what a SCADA system is • Explore security techniques used in SCADA systems • Introduce the 16 Critical Infrastructure Sectors • Kickoff team projects centered around systems within the 16 CI sectors ▪ Form teams (based on interest level) ▪ Develop a proposal and project plan
4	**Overview and Application of the Risk Management Framework (RMF)**	• Understand how to use the RMF • Explore RMF activities, tasks, and outcomes • RMF case study
5	**Security and Privacy Controls**	• Understand the fundamentals of security controls • Understand how to select security control baselines • Tailoring and creating overlays of the controls • Documenting the control selection process
6	**Overview and Application of the Cybersecurity Framework (CSF)**	• Learn to navigate and the CSF • Explore CSF activities, tasks, and outcomes • CSF case study
7	**Cyber Resiliency Considerations**	• Understand the Cyber Resiliency Engineering Framework • Understand Cyber Resiliency Goals and Objectives • Explore Cyber resiliency techniques, approaches and design principles • Cyber resiliency in the SDLC
8	**Wrapping Up Semester Projects**	• Complete the System Security Plan

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 regular homework assignments on the topics covered in class, with approximately 6 homework assignments and one semester project. There will also be weekly discussion board prompts that students are required to participate in and will be graded for. There will also be one midterm exam and a final exam. Both the midterm and the final will be given as an online, timed exam that will be available for a short window of time prior to the end of the regularly scheduled exam time. ***Note: the instructors will give students ample notice of the format, time, and any resulting stipulations about where and how the exams will be administered.***

For all group/team projects, a team evaluation will be sent to all team members to be completed on an individual and confidential basis. ***Individual grades for group/team projects will be factored by the overall average team evaluation scores received from all team members (not including the individual being scored by his/her peers) which are based on the level of individual participation, contributions, and effectiveness for the team project***. Failure to submit a team evaluation by any individual will result in the overall semester project score for that individual being reduced by 10%.

Graduate level students are required to **individually** write a report summarizing the findings of the team's semester project. This report constitutes 30% of the final grade received for the semester project. The other 70% is based on the factored team grade for the semester project.

Undergraduate students are only required to participate in the team semester project and the factored grade received for this is 100% of the individual semester project grade.

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

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

Homework Assignments:	*15%*
Class Participation (via Discussion boards on D2L):	*10%*
Knowledge Checks (short quizzes embedded in pre-recorded lectures)	*10%*
Midterm:	*15%*
Semester Project:	*30%*
Final Exam:	*20%*
Total	***100%***

Rubrics will be posted on D2L for all homework assignments the semester project.

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 is due at the time that it is specified in the course schedule and/or D2L content pages. ***Late homework and projects will not be accepted without prior approval by the instructors, and will receive 0 points.***

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

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 instructors 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.

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: http://catalog.arizona.edu/policies

Academic Integrity:
This course has a **zero tolerance policy** with respect to violations of academic integrity. Students are encouraged to share intellectual views and discuss freely the principles and applications of course materials. However, graded work/exercises must be the product of independent effort unless otherwise instructed. Students are expected to adhere to the UA Code of Academic Integrity as described in the UA General Catalog. See: http://deanofstudents.arizona.edu/academic-integrity/students/academic-integrity.

Academic Dishonesty occurs whenever any action or attempted action is pursued that creates an unfair academic advantage or disadvantage for student and/or any member or members of the academic community. All forms of academic dishonesty are subject to sanctions under the Code of Academic Integrity. Sanctions include: written warning, reduction in grade for work involved, disciplinary probation, loss of credit for work involved, failing grade in the course, suspension, and/or expulsion. Various forms of academic dishonesty include, but are not limited to cheating, fabrication, facilitating academic dishonesty, and/or plagiarism. If you are unclear what constitutes plagiarism, please ask the instructor.

Academic Misconduct is defined as any behaviors not conforming to prevailing standards or rules within the academic community. All forms of academic misconduct are subject to sanctions under the Code of Conduct. Sanctions include: restricted access to University property, administrative hold, warning, probation, suspension, and/or expulsion. Various forms of academic misconduct include, but are not limited to disruptive behavior, threatening behavior, and/or the theft or damage of University property. For more specific examples of academic dishonesty, academic misconduct, and how to avoid such behaviors, please visit the following website: http://deanofstudents.arizona.edu/tipsforavoidingacademicdishonesty

The University Libraries have some excellent tips for avoiding plagiarism available at: http://www.library.arizona.edu/help/tutorials/plagiarism/index.html.

Selling class notes and/or other course materials to other students or to a third party for resale is not permitted without the instructor's express written consent. Violations to this and other course rules are subject to the Code of Academic Integrity and may result in course sanctions. Additionally, students who use D2L or UA email to sell or buy these copyrighted materials are subject to Code of Conduct Violations for misuse of student email addresses. This conduct may also constitute copyright infringement.

Classroom Behavior Policy:
To foster a positive learning environment, students and instructors 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 Cybersecurity courses, you will primarily communicate with instructors and peers virtually through a variety of tools such as discussion forums, email, and 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.

Threatening Behavior Policy:
The UA Threatening Behavior by Students Policy prohibits threats of physical harm to any member of the University community, including to one's self. See: http://policy.arizona.edu/education-and-student-affairs/threatening-behavior-students.

UA Nondiscrimination and Anti-harassment Policy:
The University is committed to creating and maintaining an environment free of discrimination, http://policy.arizona.edu/human-resources/nondiscrimination-and-anti-harassment-policy

Our classroom is a place where everyone is encouraged to express well-formed opinions and their reasons for those opinions. We also want to create a tolerant and open environment where such opinions can be expressed without resorting to bullying or discrimination of others.

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. NIST publications). 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 instructors copyright may result in course sanctions and violate the Code of Academic Integrity.

UA Cybersecurity Student Support:
We are available to assist with **content-related** issues. You may, at any time, email us. 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. We will monitor this forum on a regular basis and 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 instructors to discuss grades or personal concerns.
- **Course Registration**: Email cybersecurity@email.arizona.edu
- **D2L Support Questions**: Email D2L@email.arizona.edu

Accessibility and Accommodations:

Our goal in this class is that learning experiences be as accessible as possible. If you anticipate or experience physical or academic barriers based on disability, please let us know immediately so that we can discuss options. You are also welcome to contact Disability Resources (520-621-3268) to establish reasonable accommodations. For additional information on Disability Resources and reasonable accommodations, please visit http://drc.arizona.edu/.

If you have reasonable accommodations, please plan to meet with one or both of us by appointment to discuss accommodations and how course requirements and activities may impact your ability to fully participate.

Students needing special accommodations or special services should contact the Disability Resources Center, 1224 East Lowell Street, Tucson AZ 85721, (520)621-3268, FAX (520)621-9423, email: drc-info@email.arizona.edu, http://drc.arizona.edu/. You must register and request that the center or DRC send the instructor official notification of your needs as soon as possible.

Please contact the instructor to discuss accommodations and how this course's requirements may impact your ability to fully participate. The need for accommodations must be documented by the Disability Resources Center.

Library Support:

The University of Arizona Libraries is dedicated to providing 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 misonline@eller.arizona.edu.

Course Surveys and Evaluations:

There are two online surveys associated with this course:

- **Cybersecurity course specific survey** - assists course designers with refining elements of the course. This survey is conducted by the Cybersecurity team prior to the end of the course.
- **UA Teacher Course Evaluation** – standard course evaluation conducted by the University of Arizona.
    - This will appear be made available through https://tce.oirps.arizona.edu/TCEOnline at the appropriate time during the course.

Please participate in these online surveys! We[1] use the comments to make changes to the course to meet student needs.

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

Subject to Change Statement:

Information contained in the course syllabus, other than the grade and absence policy, may be subject to change with advance notice, as deemed appropriate by the instructor.

Special COVID-19 Provisions

- **Classroom attendance:**
  - If you feel sick, or may have been in contact with someone who is infectious, stay home. Except for seeking medical care, avoid contact with others and do not travel.
  - Notify your instructors if you will be missing an online course.
  - Campus Health is testing for COVID-19. Please call (520) 621-9202 before you visit in person.
  - Visit the UArizona COVID-19 page for regular updates.

- **Academic advising:** If you have questions about your academic progress this semester, or your chosen degree program, please note that advisors at the Advising Resource Center can guide you toward university resources to help you succeed.

- **Life challenges:** If you are experiencing unexpected barriers to your success in your courses, please note the Dean of Students Office is a central support resource for all students and may be helpful. The Dean of Students Office can be reached at 520-621-2057 or DOS-deanofstudents@email.arizona.edu.

- **Physical and mental-health challenges**: If you are facing physical or mental health challenges this semester, please note that Campus Health provides quality medical and mental health care. For medical appointments, call (520-621-9202. For After Hours care, call (520) 570-7898. For the Counseling & Psych Services (CAPS) 24/7 hotline, call (520) 621-3334.

- **Staying current:** You are required to complete all assignments and class participation activities on your own time to accomplish.

- **Remain flexible:** If pandemic conditions warrant, the University may require that we return to remote operations. If that is the case, we will notify you by D2L Announcement and email that we are moving to remote operations.

- **Class Recordings:**
  - For lecture recordings, students must access content in D2L only. Students may not modify content or re-use content for any purpose other than personal educational reasons. All recordings are subject to government and university regulations. Therefore, students accessing unauthorized recordings or using them in a manner inconsistent with UArizona values and educational policies are subject to suspension or civil action.