FA25 SIE 573: Engineering Trustworthy Secure Systems

Course Syllabus

Primary Instructor: Bill Hayes
Email: billhayes@arizona.edu
Phone: 847-404-0136

Guest Instructor: Professor Sharon ONeal

Course Description

This course aims 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 Standards and Technology (NIST) frameworks such as the Cybersecurity 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 Cybersecurity and Infrastructure Security Agency's (CISA) 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 cybersecurity landscape, and will include the following:

1. Cybersecurity 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 the 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 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.

Textbooks:
There are no specific textbooks used for this class. However, there are numerous standards published by the National Institute of Standards and 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: Engineering Trustworthy Secure Systems - Special Publication 800-160 Volume 1.
- National Institute of Standards and Technology: Developing Cyber-Resilient Systems, A Systems Security Engineering Approach, Special Publication 800-160 Volume 2.

Other Supplemental Readings / References: *Additional supplemental materials will be referenced and provided to students via D2L.*

Course Schedule/Scheduled Topics & Activities:
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 for Systems Security Engineering**	Define key concepts and principles of Systems Security Engineering. Summarize the role of policies, standards, procedures, and guidelines in securing systems. Outline the transferable (i.e. soft) and technical skills that effective Systems Security Engineers embody.
2	**Systems Security Framework**	Define the three (3) system security engineering contexts - problem context, solution context, and trustworthiness context

		- as outlined in the System Security Engineering Framework. Identify the systems security outcomes, tasks, and activities relevant to each process outlined in the System Life Cycle - Technical, Technical Management, Organizational Project-Enabling, and Agreement.
3	**Supervisory Control and Data Acquisition (SCADA) Systems**	Provide an example of a Supervisory Control And Data Acquisition (SCADA) system. Explain security techniques used in Supervisory Control And Data Acquisition (SCADA) systems. Classify the 16 Critical Infrastructure (CI) Sectors.
4	**Overview and Application of the Risk Management Framework (RMF)**	Summarize how to use the Risk Management Framework (RMF). Explain Risk Management Framework (RMF) activities, tasks, and outcomes. Develop a risk management assessment utilizing the Risk Management Framework (RMF).
5	**Security and Privacy Controls**	Utilize the National Institute of Standards and Technology (NIST) Security Control Catalog. Select security control baselines utilizing the guidelines established by the National Institute of Standards and Technology (NIST). Customize and create overlays of security controls. Document the control selection process.
6	**Overview and Application of the Cybersecurity Framework (CSF)**	Navigate the Cybersecurity Framework (CSF). Utilize the Cybersecurity Framework (CSF) to manage activities, tasks, and outcomes. Tailor the Cybersecurity Framework (CSF) to create a security plan.
7	**Cyber Resiliency Considerations & Course Wrap-up**	Explain the Cyber Resiliency Engineering Framework.

		Interpret Cyber Resiliency Goals and Objectives. Describe Cyber Resiliency Goals and Objectives. Differentiate Cyber resiliency techniques, approaches and design principles. Prioritize Cyber resilience in the System Development Lifecycle (SDLC). 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%.

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

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

Grading Scale and Policies:

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%*
Exam 1:	*15%*
Semester Project:	*30%*
Final Exam:	*20%*
Total	***100%***

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 <u>will not</u> be accepted without prior approval by the instructors and will receive 0 points.***

AI/LLM Usage:

- Information can be found at:
- https://ucatt.arizona.edu/teaching/artificial-intelligence-teaching-learning
- **Referring to the chart below, AI can be used at Levels 1 and 2 for Assignments and Team Project (with disclosure), but at level 0 (NO AI Use) on exams, where answers must originate from our course content.**

Can I Use AI on this Assignment?

Generative AI Acceptable Use Scale

Generative AI refers to any of the thousands of Artificial Intelligence tools in which the model generates new content (text, images, audio, video, code,etc) This includes, but is not limited to, Large Language Models/ LLMs such as ChatGPT, Google Gemini,etc, Image creators such as Dall-E3, Adobe Firefly, and any tools with built in generative AI capabilities such as Microsoft CoPilot, Google Duet, Canva, etc etc)

	Level of AI Use	Full Description	Disclosure Requirements
0	NO AI Use	This assessment is completed entirely without AI assistance. AI Must not be used at any point during the assessment. This level ensured that student rely solely on their own knowledge, understanding, and skills.	No AI disclosure required May require an academic honesty pledge that AI was not used.
1	AI-Assisted Idea Generation and Structuring	No AI content is allowed in the final submission. AI can be used in the assessment for brainstorming, creating structures, and generating ideas for improving work.	AI disclosure statement must be included disclosing how AI was used. Link(s) to AI chat(s) must be submitted with final submission.
2	AI-Assisted Editing	No new content can be created using AI. AI can be used to make improvements to the clarity or quality of student created work to improve the final output.	AI disclosure statement must be included disclosing how AI was used. Link(s) to AI chat(s) must be submitted with final submission.
3	AI for Specified Task Completion	AI is used to complete certain elements of the task, as specified by the teacher. This level requires critical engagement with AI generated content and evaluating its output. You are responsible for providing human oversight and evaluation of all AI generated content.	All AI created content must be cited using proper MLA citation. Link(s) to AI chat(s) must be submitted with final submission.
4	Full AI Use with Human Oversight	You may use AI throughout your assessment to support your own work in any way you deem necessary. AI should be a 'co-pilot' to enhance human creativity. You are responsible for providing human oversight and evaluation of all AI generated content.	You must cite the use of AI using proper MLA or APA citation. Link(s) to AI chat(s) must be submitted with final submission.

Adapted by Vera Cubero for the North Carolina Department of Public Instruction (NCDPI)
from the work of Dr. Leon Furze, Dr. Mike Perkins, Dr. Jasper Roe FHEA, & Dr. Jason Mcvaugh
Link to Original Work

Creative Commons Licensed BY (attribution) NC (Non Commercial) SA (Share Alike)
To remix this for your use case, you may make an editable copy, using this TEMPLATE LINK.
Please maintain CC licensing and all attributions in all duplications, references, or remixing.

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

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.
- Compose your messages and posts in a word processing tool and check your spelling and grammar before submitting your post / email.

University-wide Policies:
Links to the following UA policies are provided here, http://catalog.arizona.edu/syllabus-policies