SP25 SIE 571 Systems Cyber Security Engineering Syllabus

Primary Instructor: Bill Hayes

Email: billhayes@email.arizona.edu

Office Hours: *TBR via Zoom*

***Guest Instructor*:** Professor Sharon ONeal

Course Description

The purpose of this course is to introduce selected topics, issues, problems, and techniques in Systems Cyber Security Engineering (SCSE), early in the development of a large system. Students will explore various techniques for eliminating security vulnerabilities, defining security specifications / plans, and incorporating countermeasures to achieve overall system assurance. SCSE is an element of systems engineering that applies scientific and engineering principles to identify, evaluate, and contain or eliminate system vulnerabilities to known or postulated security threats in the operational environment. SCSE manages and balances system security risk across all protection domains spanning the entire systems engineering life cycle. The fundamental elements of cybersecurity will be explored including: human cyber engineering techniques, penetration testing, mobile and wireless vulnerabilities, network mapping and security tools, embedded system security, reverse engineering, software assurance and secure coding, cryptography, and vulnerability analysis. After a fundamental understanding of the various cyber threats and technologies is understood, the course will expand upon the basic principles, and demonstrate how to develop a threat / vulnerability assessment on a representative system using threat modeling techniques (i.e. modeling threats for a financial banking system, autonomous automobile, or an Internet of Things device). With a cyber resilience focus, students will learn how to identify critical use cases or critical mission threads for the system under investigation, and how to decompose and map those elements to various architectural elements of the system for further analysis. Supply chain risk management (SCRM) will be employed to enumerate potential cyber threats that could be introduced to the system either unintentionally or maliciously throughout the supply chain. Additionally, the course will introduce the legal aspects of cybersecurity, including current policies and standards for legal and unlawful use of the internet and/or living in a "connected" world/society. Students will be introduced to both ethical and unethical hacking, by studying the differences between Black Hat, White Hat and Gray Hat hacking groups. The course culminates with the conduct of a Red Team / Blue Team simulation to demonstrate and explore both the attack and defend perspectives of a cyber threat. The Red Team will perform a vulnerability assessment of the prospective system, with the intention of attacking its vulnerabilities. The Blue Team will perform a vulnerability of the system with the intention of defending it against

cyber threats. Security protection planning employs a step-by-step analytical process to identify the critical technologies to be protected; analyze the threats; determine program vulnerabilities; assess the risks; and apply countermeasures. A Security Assessment Report (SAR) describes the findings of the system under analysis with the intent to mitigate risks to any advanced technology and mission-critical system functionality. Graduate students will be given an additional assignment to write a draft Security Assessment Report (SAR) for the system on which their team performed the threat analysis. Upon completion of the course, students will be proficient with various aspects of cybersecurity and how to identify system vulnerabilities early in the system engineering lifecycle. They will be exposed to various tools and processes to identify and protect a system against those vulnerabilities, and how to develop security protection plans and assessments to defend against and prevent malicious attacks on large complex systems.
This class does not teach the student "how to hack", but rather how to analyze a large, complex system early and throughout the lifecycle of the system to better protect against malicious activity and intent.

Course Prerequisites or Co-requisites

ECE 175 or instructor approval.

Course Objectives

Upon completion of this course, students will be able to address the major questions, challenges, and processes that Systems Cyber Security Engineers face, including:

1. Understanding the foundations, principles, methods and tools for developing more cyber resilient designs
2. Learning various techniques to threat model, develop system attack trees, and perform a system level vulnerability analysis
3. Understanding how the supply chain feeds into providing a cyber resilient system. Exploring techniques for managing that Supply Chain Risk and what is included in Supply Chain Risk Management (SCRM).
4. Exploring various industry standards, policies and laws related to Cyber Security principles and practices including those established by the National Institution of Standards and Technology, FedRAMP, Cloud Security Alliance and others
5. Exercise methods used in conducting a detailed Cyber Security analysis through a Blue or Red Team exercise on a self-selected commercially available product

A diverse set of topics will be covered to give students a fundamental understanding of the Cyber Security landscape, including the following:

1. Cryptography
2. Software assurance, malware and secure coding / defensive programming
3. Network mapping and security tools
4. Privacy
5. Understanding mobile and wireless vulnerabilities
6. Embedded system security
7. Human cyber engineering techniques
8. Supply Chain Risk Management
9. Fundamentals of implementing a holistic program protection planning strategy early and throughout the Systems Engineering lifecycle

10. Threat Modeling
11. Reverse engineering
12. Penetration testing
13. Ethical and Unethical Hacking
14. National Institute of Standards and Technologies (NIST) Cyber Security Framework (CSF) and Risk Management Framework (RMF)
15. Security Assessment Planning and Reports
16. Conducting various levels of Security Assessments, including Blue Team and Red Team Assessments
17. Program Protection Plans and Program Protection Implementation Plans
18. Cyber Policy and Laws

Expected Learning Outcomes

Upon completing this course, students will be able to address the major questions and issues that System Cyber Security engineers face including:

- Describe fundamental aspects of a cyber resilient system. [ABET Student Outcomes 1]
- Develop system attack trees and perform a threat and vulnerability analysis. [ABET Student Outcomes 1 and 6]
- Identify and recommend security requirements that should be part of the system security engineering activities in product development. [ABET Student Outcomes 1 and 6]
- Use tools and techniques/methodologies to analyze the vulnerabilities in a complex product or system. [ABET Student Outcomes 1 and 6]
- Describe what Information Assurance is and the role it plays in developing a cyber resilient system. [ABET Student Outcome 1]
- Describe what Software Assurance is and the role it plays in developing a cyber resilient system. [ABET Student Outcome 1]
- Evaluate how the supply chain feeds into providing a cyber resilient system and affects the cyber threat/risk posture of supplied components. [ABET Student Outcomes 1 and 6]
- Perform a security risk assessment of an Internet of Things device or other similar product. [ABET Student Outcome 7]
- Identify the differences between Ethical and Unethical Hacking (Black Hat vs White Hat Hacking). [ABET Student Outcome 4]
- Identify laws or policies in place to protect an individual or organization in the cyber domain. [ABET Student Outcome 4]
- Develop / write a System Security Plan and Security Assessment Report. [[ABET Student Outcomes 3 and 5]
- Conduct a Red Team / Blue Team assessment in a collaborate group project / simulation. [ABET Student Outcomes 5]
- Work in teams to solve a larger problem and communicate findings with peers and technical experts from diverse engineering backgrounds. [ABET Student Outcomes 5 and 7]

Course Modality

For MS students that are registered as **"AZ Online"**, the course will be run via an **Asynchronous Online format.**

Course Format and Teaching Methods

This course is structured around recorded lectures and discussions on topics that are covered in those lectures. We will also have several guest lectures from industry that are invited to share their experiences and perspectives on various Cyber topics.

There will be a separate content section for each week of the course in D2L. For each week, there will be a summary of the reading assignments, homework assignments, and key objectives. There may also be several additional reading resources posted for that week within that content folder. For each week, different discussion questions will also be posted to extend the learning by sharing with your classmates. These are very interesting and provide different thought-provoking perspectives and experiences.

Students should watch the lectures that have been recorded in the UA Studio. Learners are also required to interact with their classmates through the various discussion forum topics.

Students will take exams online, within a specified window of time that will be given by the instructor and can be found on the Course Site in D2L.

All students should:

- Check D2L regularly.
- Turn-in assignments by due date/time (allow for D2L "glitches").
- Treat instructors, speakers and peers with respect.
- Always behave in an ethical manner.
- All students are required to abide by the Student Code of Academic Integrity: http://dos.web.arizona.edu/uapolicies
- Threatening behavior by students is strictly prohibited. For detailed information see: http://policy.web.arizona.edu/~policy/threaten.shtml.

Online students:

View recorded lectures in a timely manner, per the course schedule found in D2L.

Note: **DUE DATES** for course deliverables are all posted on D2L.

Course Time Zone

All dates and times 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

Class Participation Policy

Participating in this course is vital to the learning process. As such, participation in class discussions via discussion boards on D2L is required. As such, participation in class discussions on D2L is required and will be factored into the final grade.

Please send an email to the instructor to request a homework assignment or exam extension for a valid reason (these include extended illness, death in the family, or conflict with a work commitment. **Extensions will not be given because of workload or exams in other classes.**

Course Communications

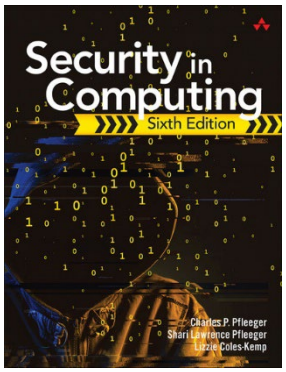
For questions that could benefit all classmates, please use the **Ask the Instructor** discussion forum on D2L to contact the instructor for content related questions. By using this means of communicating, all students can see the response and benefit from the learning as well. If you have a question regarding your personal performance in the course, please email the instructor directly or make an appointment to discuss your any concerns you have about the class. Under normal circumstances, the instructor will respond within 24 hours of your email or posting on any day of the week. When appropriate, the instructor will provide feedback on course work that needs to be manually graded (e.g., papers, assignments) within 72 hours of submission. You will be able to see the results for automatically graded course work after the specified deadline.

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. I will use D2L for course assignments, content distribution, and important announcements. The University of Arizona's D2L system is available at: http://D2L.arizona.edu.

Required Texts or Readings



Pfleeger, C., Pfleeger, S., and Coles-Kemp L., Security in Computing, 6th Edition, Prentice-Hall, 2023

Security in Computing, 6th Edition (oreilly.com)

Other Required or Special Materials

You will need a computer with Microsoft Office or equivalent and the ability to log into D2L. For the semester project, you will also likely need access to various team collaboration tools to facilitate team sharing and work products being generated. Those tools can be agreed to by the team at the start of their project.

Assignments and Examinations: Schedule/Due Dates

There will be weekly assignments and discussion participations that all students will be expected to complete, one team project (Red Team/Blue Team Simulation), one midterm and a final exam. The schedule for all these course deliverables will be provided at the start of the semester and will be posted on the Course Calendar section of D2L. The due dates are subject to change and ample notice will be given to students when any change does occur. However, it is the student's responsibility to check and monitor the completion of all assignments**.** ***IN GENERAL, NO LATE WORK WILL BE ACCEPTED.***

Graduate students will develop a Security Assessment Report (SAR) based on the findings of their team project - either a Red Team or Blue Team (RTBT) Simulation. The grade for these documents will be factored into their overall grade for the team project. The instructor will go over the weighting of all aspects of the team project for both BS and MS students in class when the project is assigned.

Grades will be assigned as measures of performance on required activities. Rubrics will be made available for all assignments.

For the team project, all students will be required to individually submit 1 Team evaluation for all deliverables for the RTBT Simulation project. **An individual student's final team project grade will be factored by the average score of all team members' inputs from these evaluations.** Every team member is expected to contribute equally to the project. If there are team dynamics that are preventing a collaborative working environment, it is best to inform the instructor ahead of time so that adjustments can be made to facilitate effective teaming and communication amongst the team.

The grading distribution for course assignments, class participation, projects, and exams are as follows:

Class Participation (Discussions):	15%
Cyber News Discussion Board:	5%
Weekly Assignments:	15%
Midterm Exam:	15%
Red Team / Blue Team Simulation:	25%
Final Exam:	25%
Total	***100%***

Late Work

In general, late work will not be accepted. ***Late homework and projects will not be accepted, and the student will receive 0 points for any missed or late work.***

Caveat: Should you encounter a serious/significant unanticipated or uncontrollable event that may prevent you from meeting a deadline, contact the instructor immediately to request an extension. Extensions are not automatic or guaranteed. All extensions must be requested at least 48 hours in advance.

Quality of Work Expectations

Two of the outcomes for this course is to collaborate on teams and communicate effectively with people from diverse technical backgrounds. This requires that one take personal pride in their work and be held accountable for timely and professional quality work. To this end, the following quality expectations are established for this course:

- For all out-of-class work, organization, presentation style, grammar, and spelling will be weighted into the score. Spelling will be evaluated using the Microsoft *Word* Standard United States dictionary.
- **All assignments will be scanned by the TurnItIn plagiarism tool and any assignments that have a score higher than 15% on any homework assignment or exam response, will receive a 0% on the assignment.** If you are using different sources/references you find online, then please document or reference that part of the text appropriately.

- Points will be lost for poorly organized or unprofessional work. This includes spelling and grammar errors, poor word choice, and poor sentence structure.

- Points will be lost for not following instructions.

- Students who have writing difficulties or deficiencies, and students for whom English is a foreign language should consider using the services provided for free through the University of Arizona Writing Laboratory

Feedback on Submitted Work

For the purposes of this section, feedback refers to the scored assessment of learning on any given assignment, examination, project or paper. Scores are summed, categorized, and weighted to determine the final course grade. The following policies apply to scores:

- Feedback will be provided regularly by your instructor – as quickly as possible. Every instructor has multiple responsibilities beyond his/her courses. And each instructor has a unique way of providing feedback. If you believe you are not getting enough feedback, you are encouraged to contact your instructor and ask for more.

- The instructor will make every effort to grade assignments within 72 hours, but no later than one calendar week after the assignment due date.

- To comply with federal privacy law (specifically, FERPA), graded materials will never be passed around the classroom, or placed in any publicly accessible location, physical or online. Most scored work will be returned via D2L directly to the named student or student team.

- Any student wishing to appeal any given score must return his or her graded work with a written statement explaining the appeal. An appeal must be submitted no later than one calendar week after the original score was posted. Any work submitted for re-grading will be graded in its entirety.

Final Examination

Online students will be provided instructions on how and when to take the exam asynchronously online. T here will be a window of time that the exam is active. S tudents must make arrangements to make themselves available to take the exam within that window of time.

Details for how the exam will be administered will be provided at a minimum of 2 weeks prior to the Final Exam date. *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.*

The University's Final Exam Schedule can be found at
http://www.registrar.arizona.edu/schedules/finals.htm

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 why 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.

Grading Scale and Policies

The following scale will be used to award the final grades, for both 400 / 500 students:

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

A rubric will be made available on D2L for all deliverables for the course.

Dispute of Grade Policy: Any disputes for a grade on one of the course deliverables must be made within 1 week of receiving the grade.

Scheduled Topics/Activities

The course schedule and due dates will be maintained online at D2L. Please refer to D2L often for any changes that may be made throughout the semester.

Other Course Policies

Online Collaboration/Netiquette

In this course, you will primarily communicate with the instructor and peers through a variety of tools such as discussion forums, 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 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/educati9on-and-student-affairs/disruptive-behavior-instructional-setting
- Compose your messages and posts in a word processing tool and check your

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 (except for 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. Violations of the instructor's copyright may result in course sanctions and violate the Code of Academic Integrity.

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 concerns.
- **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