THE UNIVERSITY OF ARIZONA

SIE 471 / 571 Systems Cyber Security Engineering Syllabus

Description of Course

The purpose of this course is to introduce selected topics, issues, problems, and techniques in System 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 system 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 system engineering life-cycle. The fundamental elements of cyber security 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 are 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 cyber security, 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 realistic 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. For teams that select the same system to analyze, a comparison will be made between the outcomes of both the Red team and the Blue Team to better understand the overarching solutions to addressing the threats identified. 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 that their team performed the threat analysis for.

Upon completion of the course, students will be proficient with various elements of cyber security 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 assessment 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 System 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. 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:

- What are fundamental aspects of a cyber resilient system?
- How is a threat and vulnerability analysis performed? How do you develop a system attack tree?
- At what point in the systems engineering lifecycle should a system architect begin building in cyber resiliency?
- What tools and techniques are used to analyze the vulnerabilities in a system?
- What does Information Assurance mean and what role does it play in developing a cyber resilient system?
- What does Software Assurance mean and what role does it play in developing a cyber resilient system?
- How does the supply chain feed into providing a cyber resilient system? How do you manage that risk with the supply chain?
- What are the differences between Ethical and Unethical Hacking (Black Hat vs White Hat Hacking)?
- What laws or policies are in place to protect an individual or organization in the cyber domain?
- How do you develop a viable and affordable program protection plan to ensure system assurance?
- How do you conduct a Red Team / Blue Team simulation?
-

Additionally, students will learn to work on teams to solve a larger problem and will also be given the opportunity to communicate with peers and technical experts from diverse engineering backgrounds.

Course Operation

This course is structured around interactive lectures and discussion on the 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 throughout the semester. These guest lectures are extremely interesting and engaging.

The covered topics are grouped into "Modules". There will be a separate content section for each module on D2L. Within that module, there will be a summary of the reading assignments, homework assignments, and key objectives of the module. There may also be several additional reading resources posted for that module within that content folder. For each module, 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.

Online students can watch lectures that have been filmed during the normal class time and it is strongly recommended that you watch all the videos to hear the real time commentary and interactions between the instructor and the class. Online students are also required to interact with their classmates through the various discussion questions posted for each module.

All exams will be given in real time for on campus students. Online students will have the opportunity to take exams online within a specified window of time that will be given by the instructor.

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.

On-campus students:

- Arrive on-time, turn off cell phones, beepers, social networks, etc.
- Attend class regularly and participate in class discussions and activities.

Online students:
View lectures in a timely manner, preferably within 48 hours of the lecture date.

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

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

Absence and Class 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

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

Participating in this course and attending lectures and other course events are vital to the learning process. As such, attendance and participation are required at all lectures and on discussion boards on D2L. Students are responsible for all materials and discussions covered during class. As such, attendance and participation in class discussions on D2L is required and will be factored into the final grade at a factor of 20%. Students who miss more than 1 class contiguously due to illness or emergency are required to bring documentation from their health-care provider or other relevant, professional third parties for the absences to be excused. Failure to submit third-party documentation will result in unexcused absences.

Please send an email to the instructor if you are going to miss class to ask for an excused absence **in advance of the class**. If advanced notice is given for a good reason, then your absence on that day *MAY* be excused. Examples of good reasons include: traveling to an interview, traveling out of city for an important family event (like a wedding), or being ill. **Absences will not be excused because of workload or exams in other classes.**

Attendance at all Red Team / Blue Team Simulation Out-briefs is an especially important part of the learning in this class and any unexcused absence on those days will result in your individual score for the team project being lowered by 5pts for each day of absence. If you have an unexcused absence for your own Red Team / Blue Team simulation out-brief, it will result in you receiving a failing grade for your project. There will be no excused absences for those class sessions without a Dean's excuse or documentation from a health care provider.

Course Communications

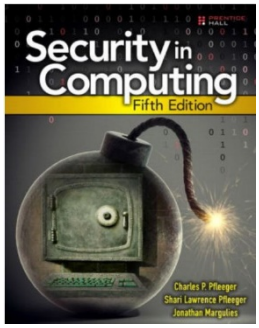
For questions that could benefit all classmates, please use the **Ask the Instructor** discussion forum on D2L to contact the instructor for content related questions. By using this means of communicating, all students can see the response and benefit from the learning as well. If you have a question 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 (quite often sooner). 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 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 Margulies, J., Security in Computing, 5th Edition, Prentice-Hall, 2015

Other Required or Special Materials

You will need a computer with Microsoft Office or equivalent and the ability to log into D2L. For the term 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 have an additional assignment to develop a draft Security Assessment Report (SAR) based on the findings of their team project - either a Red Team or Blue Team 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.

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

Class Participation / Discussion Boards	20%
Module 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 secondary 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 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 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

The Final Exam is scheduled for Wednesday, December 12th from 10:30 – 12:30 in our regular classroom. Online students will be provided instructions on how and when to take the exam online. For online students, there will be a window of time that the exam is active (typically starting at the same time the exam is active for on campus students). Online students must make arrangements to make themselves available to take the exam within that window of time.

At the discretion of the instructor, both the midterm and the final may 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 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 Regulations can be found at https://www.registrar.arizona.edu/courses/final-examination-regulations-and-information, and Final Exam Schedule can be found at http://www.registrar.arizona.edu/schedules/finals.htm

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.

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.

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.

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.).

Students are asked to refrain from disruptive conversations with people sitting around them during lecture. Students observed engaging in disruptive activity will be asked to cease this behavior. Those who continue to disrupt the class will be asked to leave lecture or discussion and may be reported to the Dean of Students.

Threatening Behavior Policy

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

Online collaboration / Netiquette

In some of your coursework, you will primarily communicate with 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.

Accessibility and Accommodations

At the University of Arizona we strive to make learning experiences as accessible as possible. If you anticipate or experience physical or academic barriers based on disability or pregnancy, you are welcome to let me know so that we can discuss options. You are also encouraged to contact Disability Resources (520-621-3268) to explore reasonable accommodation.

If our class meets at a campus location: Please be aware that the accessible table and chairs in this room should remain available for students who find that standard classroom seating is not usable.

Code 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.

The University Libraries have some excellent tips for avoiding plagiarism, available at http://new.library.arizona.edu/research/citing/plagiarism. The instructor will be using online plagiarism detection tools that will indicate the total amount of material that is pulled from published resources. More than 10% on any given assignment will adversely impact your grade for the assignment and may result in a failing grade.

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 e-mail to sell or buy these copyrighted materials are subject to Code of Conduct Violations for misuse of student e-mail addresses. This conduct may also constitute copyright infringement.

UA Nondiscrimination and Anti-harassment Policy

The University is committed to creating and maintaining an environment free of discrimination; see 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.

Additional Resources for Students

UA Academic policies and procedures are available at http://catalog.arizona.edu/policies

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/personal-information/family-educational-rights-and-privacy-act-1974-ferpa?topic=ferpa

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.