Fall 2017 **SIE 471/571 Systems Cyber Security Engineering**

On-campus Students:
M W F 11:00am – 11:50am

Distance Ed Students:
Access lecture video recordings through Content page of D2L

Sharon O'Neal
sharononeal@email.arizona.edu

Office Hours: Tues and Thurs 2:00 – 3:30pm
or by appointment (please feel free to call or email at any time)

Course Description:

The purpose of this course is to introduce selected topics, issues, problems, and techniques in the area of 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 in order 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, vulnerability analysis, and cyber forensics. 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 a power distribution system). 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 in order to better understand the overarching solutions to addressing the threats identified. Graduate students will be given an additional assignment to write a draft Security Assessment Plan (SAP) and Security Assessment Report (SAR) for the system that their team performed the threat analysis for. 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 SAP describes the findings of the system under analysis with the intent to mitigate risks to any advanced technology and mission-critical system functionality.

Upon completion of the course, students will be proficient with various elements of cyber security and how to identify system vulnerabilities early on 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 Prerequisite(s): ECE 175 or instructor approval

Course Format and Course Communication:

This course is lecture based. This class will use web-based D2L (Desire to Learn) as the only means of distributing class materials including assignments and exams. All Projects and Homework must be uploaded into D2L Dropboxes on or before the due dates. **No late assignments will be accepted.** Your grades for this course will also be available on D2L. You will need a UANet ID to access D2L at the following site: http://d2l.arizona.edu/. You are expected to check D2L ***frequently*** for class information and to participate in online discussions relative to the course materials.

Course Objectives and Learning Outcomes:

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 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. Cryptography
2. Software Assurance, Malware and secure coding / defensive programming
3. Network mapping and security tools
4. Information Assurance
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. Developing threat and vulnerability assessments and attack trees for a large system
12. Reverse engineering
13. Digital forensics
14. Penetration testing
15. Ethical and Unethical Hacking
16. National Institute of Standards and Technologies (NIST) Cyber Security Framework (CSF)
17. Conducting various levels of Security Assessments, including Blue Team and Red Team Assessments
18. Program Protection Plans and Program Protection Implementation Plans
19. Security Assessment Planning and Reports
20. Cyber Policy and Laws

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?

Absences 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 the course and attending lectures and other course events are vital to the learning process. Students are responsible for all materials covered during class. As such, attendance and participation in class discussions on D2L is strongly recommended, and will be factored into the final grade at a factor of 20%. Occasionally, attendance may be ***required*** for special events such as final project presentations. Students who miss class due to extended illness or emergency are required to bring documentation from their health-care provider or other relevant, professional third parties. Failure to submit third-party documentation will result in unexcused absences.

Class Guidelines:

All students:

- 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.

Distance Ed students:

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

Required Textbook:

Pfleeger, C., Pfleeger, S., and Margulies, J., Security in Computing, 5th Edition, Prenticee-Hall, 2015.
Shostack, A., Threat Modeling: Designing for Security, Wiley, 2014.

Required Materials: Microsoft Office and Clickers for class participation (available at the UofA Bookstore). *Online students are not required to have clickers, but may take "assessments" to check their own understanding of the lectures and material covered through D2l and Panopto.*

Required Extracurricular Activities:

None

However, there will be *optional opportunities* to participate in various community and statewide Cyber events as the community calendars permit. Students will be encouraged to participate in the UofA CyberCats club events, and optimistically be given the opportunity to learn more about the Arizona Cyber Range in the greater Phoenix area.

Assignments and Examinations:

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.

Graduate students will have an additional assignment to develop a draft Security Assessment Plan (SAP) and a Security Assessment Report (SAR) based on their team project (the grade for these documents will be factored into their overall grade for the team project – either a Red Team or Blue Team Simulation.

Final Examination:

The Final Exam is scheduled for Wednesday, December 13th from 10:30 – 12:30 in the regular classroom. 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 grades will be distributed as follows:

Class Participation	15%
Discussion Boards / Module Assignments:	20%
Midterm Exam:	15%
Red Team / Blue Team Simulation:	25%
Final Exam:	25%

Final Grades for this course will be computed as follows:

>90%	A
>80%	B
>70%	C
>60%	D
<60%	E

Percentages will not be raised to achieve the above grades. However, the percentages may be lowered based on statistical analysis of class performance.

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.

Scheduled Topics/Activities:

The SIE 471/571 Class Schedule is available on D2L. It lists all material to be covered by date and includes references to the textbook chapters. All assignments are listed with their respective due dates. **Note that the Dropbox for each assignment will remain open only until Midnight the day the assignment is due.**

All homework/projects/presentations and papers are to be submitted by the due date/time to the D2L Dropbox unless otherwise specified. All D2L activities, including Discussions, Assignments and Exams must be complete by the due date/time. **No late work is accepted.** No extra credit is available.

The grades for SIE 471/571 will be distributed as follows:

Discussions / Weekly Assignments: within 3 days of due date
Class Participation: no later than December 12thth
Red Team / Blue Team Simulation: no later than December 8th
Midterm Exam: no later than October 13th
Final Exam: no later than December 14th

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.).

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.

Accessibility and Accommodations:

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

If you have reasonable accommodations, please plan to meet with me by appointment or during office hours to discuss accommodations and how my course requirements and activities may impact your ability to fully participate.

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://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 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:

All student records are held in strict confidence. Additional information can be found at http://www.registrar.arizona.edu/personal-information/family-educational-rights-and-privacy-act-1974-ferpa?topic=ferpa

Subject to Change Statement:

The information contained in the course syllabus, other than the grade and absence policies, may be subject to change.