Course Syllabus

Instructor: Sharon ONeal

Email: sharononeal@email.arizona.edu

Teaching Assistant: N/A

Email: N/A

Course Description

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, 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 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.

Textbooks: ***Security in Computing***, 5th Edition,
Pfleeger, C., Pfleeger, S., and Margulies, J., Prentice-Hall, 2015.

Threat Modeling: Designing for Security, Shostack, A., Wiley, 2014.

References: *Several supplemental materials will be referenced and provided to students via D2L.*

Prerequisites: 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 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

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

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?

Course Operation

This course is structured around weekly progress. 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 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

Office Hours and Communications:

Please use the **Ask the Instructor** discussion forum on D2L to contact me for content related questions. All students can then benefit from my response. Under normal circumstances, I will respond within 24 hours of your post 7 days of the week (quite often sooner). If you have a question regarding your personal performance in the course, please email me directly using the address above. When appropriate, I 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 (online quizzes and exams) 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, 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 weekly homework assignments on the topics covered in class, with approximately 4 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 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.

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

Homework Assignments:	15%
Class Participation (via Discussion boards on D2L):	15%
Midterm:	20%
Projects:	25%
Final Exam:	25%
Total	***100%***

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 homework handout and/or D2L content pages (all homework handouts will be posted on D2L). ***Late homework and projects will not be accepted, and will receive 0 points.***

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 instructor 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.

Absence and Class Participation Policy

Participating in course is vital to the learning process. As such, timely participation in online discussions and/or any team projects is absolutely required. Students who miss deadlines due to illness or emergency are required to provide documentation from their healthcare provider or other relevant, professional third parties. Failure to submit third-party documentation will result in unexcused absences and result in lowered participation grades. The UA's policy concerning Class Attendance, Participation, and Administrative Drops is available at: http://catalog.arizona.edu/2015-16/policies/classatten.html.

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: http://uhap.web.arizona.edu/policy/appointed-personnel/7.04.02

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.

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. 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:

I am available to assist with **content-related** issues. You may, at any time, email me. 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. I 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 instructor 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 me 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 me by appointment or during office hours to discuss accommodations and how my 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 me. 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! I 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.