UNIVERSITY OF ILLINOIS URBANA-CHAMPAIGN

The Grainger College of Engineering
Information Trust Institute

ENG 298: Foundational Technical and Organizational Concepts and Practices in Cybersecurity
Fall 2024 Syllabus

CRN: 53549
Course Dates: August 26 - December 11, 2024
Credits: 3
Prerequisites: CS 124, or ECE 120, or IS 401, or instructor approval
Meeting Time: Online (synchronously), Tuesdays 5:00-7:50pm
Instructor: Casey W. O'Brien, Associate Director, Cyber Defense Education and Training, Information Trust Institute (ITI)
Office: Coordinated Science Lab (CSL) 449
Email: cwobrien@illinois.edu
Phone: 217-265-7689
Office Hours: By appointment only

Overview

This 15-week, 3 credit survey course introduces the learner to the current risks and threats to an organization's users, systems, and data, combined with structured tactics, techniques, and procedures (TTPs) for addressing the safeguarding of these critical assets. The course also provides a foundation for those new to cybersecurity by delivering the broad-based knowledge and skills necessary to prepare students for further study in other specialized cybersecurity courses/fields/domains.

Course Topics

This course will provide an overview of core concepts that are part of the following topics:

- Module 1: Defining Cybersecurity
- Module 2: Threats, Attacks, and Vulnerabilities
- Module 3: Governance, Risk, and Compliance (GRC)
- Module 4: Identity and Access Management (IdAM)
- Module 5: Physical Security
- Module 6: Cryptography and Public Key Infrastructure (PKI)
- Module 7: Security Engineering
- Module 8: Security Testing
- Module 9: Security Operations

Expected Course Outcomes

Upon completion of this course, students will be able to:

- Discuss the nature and consequences of vectors of disruption in cyber-social systems.
- Describe why cybersecurity is essential in today's enterprise environments.
- Develop a threat model given an organization's assets, risks, and adversaries.
- Identify the elements that make up an organizational security policy. Describe the measures needed to implement and enforce it.
- Recognize how an enterprise infrastructure is monitored.
- Operate with an awareness of applicable laws and policies, including principles of governance, risk, and compliance.
- Identify common attacks and describe how to safeguard against them.
- Develop an information security program for a fictitious company, leveraging cybersecurity

frameworks and standard operating procedures.
- Implement Asymmetric and Symmetric cryptography, hashing, and a public key infrastructure.
- Describe how systems and services can be hardened.

Learning Resources
- All required material (e.g., narrated video lectures, readings, and labs) will be provided to students, as per the tentative schedule below.
- Campus resources (e.g., library, counseling, advising) provided as currently to online students.
- Lab Environments: This course leverages online, hands-on lab environments, used to deliver the software and related tools/files, which are necessary components to not only completing the lab assignments, but also to help the learner develop their knowledge and skills.

Assignments
The course's instructional content will be made available via **Canvas**, a web-based Learning Management System (LMS), that allows institutions to manage digital learning, educators to create and present online learning materials and assess student learning, and students to engage in courses and receive feedback about skill development and learning achievement. Course site:

https://canvas.illinois.edu

Each week's module may contain the following (not all weeks have the same assignments):
- Due dates.
- Learning objectives for that week's module.
- Required and supplemental (optional) reading material.
- Links to supplemental materials.
- Video(s).
- Discussion topic.
- Quiz.
- Hands-on lab assignment(s).
- Extra credit assignment(s).
- List of concepts/glossary of terms.

9 Quizzes (180 total points)
Tech-related courses (and the related fields in general) are full of jargon and acronyms; you must learn this language if you are to be successful in this class, and/or the field in general. There is no shortcut around this. However, instead of memorizing and regurgitating facts that can be easily looked up, you will create the module 1-9 quizzes. Research shows that information is better remembered if it is generated by the learner rather than simply read, known as the *generation effect*. The quiz questions (10 total per module) should be a combination of multiple-choice, true/false, and fill in the blank. These questions are to be generated from each module's list of concepts (at the end of each module). You are allowed to use any resource at your disposal to create these questions. Each submitted quiz is 20 points each. See the Quiz assignment in each Canvas module for more on this.

10 Discussions (200 total points)

You will be required to participate in weekly, online discussions using the Discussions feature in Canvas. Each “posting” helps you analyze one aspect of the methodological, theoretical, or disciplinary perspective based on that week’s topic, or a set of related core concepts, and respond to at least one others’ post. You are encouraged to use any resource at your disposal to complete these assignments. If you do use external resources (e.g., websites, textbooks, ChatGPT, etc.), be sure to cite your sources using the American Psychological Association (APA) 7th edition format. Also, feel free to include curated media elements (e.g., videos, infographics, images, attached documents, etc.). Each post is 20 points each.

14 Lab Assignments (280 total points)

The hands-on lab assignments are designed to reinforce the concepts covered in the reading material, as well as to help you develop your knowledge and skills. In addition, extra credit assignments may be given during the semester. Students should do the extra credit, which is fun and designed to be challenging.

Grading Summary

Grades are assigned based on the grading policy stated in this syllabus, as follows:

Assignments	Points Possible for Each Activity	Total Points Possible
Quizzes	20 points each (x9)	180
Discussions	20 points each (x10)	200
Lab Assignments	20 points each (x14)	280
Extra Credit	TBD	TBD
	Total >>	660

Grading Policy

A+	=	100 - 96%
A	=	95 - 93%
A-	=	92 - 90%
B+	=	89 - 87%
B	=	86 - 83%
B-	=	82 - 80%
C+	=	79 - 77%
C	=	76 - 73%
C-	=	72 - 70%
D+	=	69 - 67%
D	=	66 - 63%
D-	=	62 - 60%
F	=	Below 60%

ENG 298: Foundational Technical and Organizational Concepts and Practices in Cybersecurity
Fall 2024 Syllabus

Course Policies

- Late assignments: 20% penalty per week.
- Attendance: Online synchronous classes.
- Generative AI usage policy: If you decide to use Generative AI through publicly available interfaces (e.g., ChatGPT), as well as being extremely cautious of their deficiencies for scholarly work, you are required to provide:
    1. Your prompt(s),
    2. The output text, with before/after highlighted (e.g. use “compare documents” in Word), and,
    3. A change note analyzing your experience of advantages and disadvantages in use.

Contacting the Instructor

The best way for students to reach the instructor is via email, who will typically respond to student emails within 24-48 hours.

Equal Opportunity and Access

To obtain disability-related academic adjustments and/or auxiliary aids, students with disabilities must contact the course instructor and the Disability Resources and Educational Services (DRES) as soon as possible. To contact DRES you may visit 1207 S. Oak St., Champaign, call 217-333-4603 (V/TDD), or e-mail disability@uiuc.edu.

To ensure that disability-related concerns are properly addressed from the beginning, students with disabilities who require assistance to participate in this class are asked to see the instructor as soon as possible.

If you need accommodations for any sort of disability, please contact the instructor.

Wellness

Significant stress, mood changes, excessive worry, substance/alcohol misuse or interferences in eating or sleep can have an impact on academic performance, social development, and emotional wellbeing. The University of Illinois offers a variety of confidential services including individual and group counseling, crisis intervention, psychiatric services, and specialized screenings which are covered through the Student Health Fee. If you or someone you know experiences any of the above mental health concerns above, it is strongly encouraged to contact or visit any of the University’s resources provided below. Getting help is a smart and courageous thing to do – for yourself and for those who care about you.

- Counseling Center (217) 333-3704
- McKinley Health Center (217) 333-2700
- National Suicide Prevention Lifeline (800) 273-8255
- Rosecrance Crisis Line (217) 359-4141 (available 24/7, 365 days a year)

- Anonymous Suicide Incident Referral Form: http://www.counselingcenter.illinois.edu/counseling/counseling-center-policies/suicide-intervention-policy.

Academic Integrity
The Illinois Student Code should also be considered as a part of this syllabus. You should pay particular attention to Article 1, Part 4: Academic Integrity. Read the Code at the following URL: https://studentcode.illinois.edu.

Academic dishonesty will result in a failing grade. Every student is expected to review and abide by the Academic Integrity Policy: https://studentcode.illinois.edu. Please note, you are responsible for reading this policy. Ignorance is not an excuse for any academic dishonesty.

Emergency Planning
Plan for emergency situations by reviewing the important material found at https://police.illinois.edu/em. The more prepared you are, the safer you will be.

Tentative Schedule (subject to change)

Weeks	Modules	Due Dates
1-2: Aug. 27 - Sep. 9	- **Module 0**: Getting Started - **Module 1**: Defining Cybersecurity	Sep. 9
3-4: Sep. 10-23	- **Module 2:** Threats, Attacks, and Vulnerabilities	Sep. 23
5: Sep. 24-30	- **Module 3:** Governance, Risk, and Compliance (GRC)	Sep. 30
6: Oct. 1-7	- **Module 4:** Identity and Access Management (IdAM)	Oct. 7
7: Oct. 8-14	- **Module 5:** Physical Security	Oct. 14
8-11: Oct. 15 - Nov. 11	- **Module 6:** Cryptography & Public Key Infrastructure (PKI)	Nov. 11
12-13: Nov. 12-22	- **Module 7:** Security Engineering	Nov. 22
14: Nov. 23 - Dec. 1	**NO CLASS: FALL BREAK**	
15: Dec. 3-9	- **Module 8:** Security Testing	Dec. 9
16: Dec. 10-12	- **Module 9**: Security Operations	Dec. 17
December 13-19	**FINALS WEEK**	
December 18	**GRADES SUBMITTED BY 12 PM**	