University of Maine
School of Computing and Information Science

Course Name: Introduction to Cybersecurity **Number:** COS430/530 **Semester:** Spring 2024
Classroom: Estabrooke Hall 130 **Class Hours:** 11:00 AM – 12:15 PM (Tu/Th)

Instructor: Sepideh Ghanavati **Office:** Boardman Hall 234 **Email:** sepideh.ghanavati@maine.edu
Instructor Office Hours: Thursdays 12:30 PM – 1:30 PM or by appointment.

TA: Shuvra Smaran Das **TA-Office:** 138 Boardman Lab **TA-Email:** shuvra.das@maine.edu
TA-Office Hours: Mondays 10 AM – 2:00 PM

Catalogue Listing: Theory and practice for cybersecurity. Topics include authentication, access control, cryptography, software, and web security, security operations, risk and incident management, network security, legal, ethics and privacy issues, and emerging technologies.

Reading Materials (required): The main textbook of the course is:
Security in Computing – 6th Edition – Ch. P. Pfleeger, Sh. Lawrence Pfleeger, J. Margulies – 2024.
Chapters to read will be mentioned every week, under the mandatory part.

Reading Materials (optional): The optional/complementary textbooks of the course are:
Computer & Internet Security – A hands-on Approach – 2nd Ed. – Wenliang Du – 2019.
Computer Security: Principles and Practice – 5th Edition – William Stallings, Lawrie Brown – 2024.
Cryptography and Network Security: Principles and Practice – 8th Edition – William Stallings, 2020.

All other required reading lists will be provided in another document. The instructor will include the required reading material from the list at the end of each lecture presentation.

Course Prerequisites: COS 331.

Expected prior knowledge and skills in: The successful student should have knowledge of Python and/or C programming and should be familiar with basic networking, operating system, and database concepts.

Key Topics:

1. Authentication and Access Control
2. Introduction to Cryptography
3. Secure Software Development
4. Database and Web Security
5. Communication and Network Security
6. Security Operations
7. Risk and Incident Management
8. Legal Issues, Ethics and Privacy

Course objectives:
The purpose of this course is to introduce advanced cybersecurity theories, methods, and tools. Upon successful completion of this course, students will be able to:

- Apply security principles and practices to the design, implementation, and operations of the physical, software, and human components of the system as appropriate to the program.
- Analyze and evaluate components and systems with respect to security and to maintaining operations in the presence of risks and threats
- Consider legal, regulatory, privacy, ethics, and human behavior topics as appropriate to the program.

More specifically, students will be able to:

- State the basic concepts of information security, including security policies, security models, and security mechanisms.
- Explain concepts related to applied cryptography, including plaintext, cipher-text, the four techniques for crypto-analysis, symmetric cryptography, asymmetric cryptography, digital signature, message authentication, code, hash functions, and modes of encryption operations.
- Explain the concepts of malicious code, including viruses, Trojan horses, and worms.
- Explain common vulnerabilities in computer programs, including buffer overflow vulnerabilities, time-of-check to time-of-use flaws, and incomplete mediation.
- Outline the requirements and mechanisms for identification and authentication.
- Explain issues about password authentication, including dictionary attacks (password guessing attacks), password management policies, and one-time password mechanisms.
- Explain and compare security mechanisms for conventional operating systems, including memory, time, file, and object protection requirements and techniques and protection in contemporary operating systems.
- Explain the requirements for trusted operating systems, and describe the independent evaluation, including evaluation criteria and evaluation process.
- Describe security requirements for database security, and describe techniques for ensuring database reliability and integrity, secrecy, inference control, and multi-level databases.
- Describe threats to networks, and explain techniques for ensuring network security, including encryption, authentication, firewalls, and intrusion detection.
- Explain the requirements and techniques for security management, including security policies, risk analysis, and physical threats and controls.

Learning Outcomes & Assessment Methods:

Students who have completed this course should have the ability to:

Objectives	ABET Outcomes	Assessment Methods
1. Understand security principles and practices.	1	D, A, PP, SR
2. Analyze and evaluate components and systems with respect to security principles and practices.	1	D, A, PP, SR
3. Perform risk and threat assessment.	1	D, A, PP, SR
4. Understand legal, regulatory, privacy and ethical topics.	4	D, A, PP, SR
5. Working Effectively in teams.	5	PP, SR

Activities and Evaluation:

Students' performance will be evaluated based on class participation/discussions, assignments, security reports, and programming projects.

- **Lectures** – There will be 150 minutes of lectures every week, Tuesdays, and Thursdays, in which students will learn about topics in cybersecurity.
- **Readings** – Students will be assigned readings from the course textbook or academic papers to learn and establish methods based on a strong engineering foundation.

- **(D) – In-Class Participation and Discussions on Discord (10%) –** Students reflect on reading materials and discussions in the class as well as on COS430/530 Discord channel. Note that, **active participation** is **required**, either in class, on Discord, or both. Discussions are **individual** assessments.
- **(A) – Assignments (30%)** – Students have 3 take-home assignments during the semester whereby students apply methods taught in class to sample problems. Each assignment is worth 10%. All assignments are **individual** efforts.
- **(SR) - Security Reports (20%) –** Students, **in a group of 2**, will write 4 security reports related to the Common Weakness Enumerations (CWE) and present a summary to the class. The details of these reports are given in another document and will be posted on Brightspace. **Graduate students (i.e., COS530) will complete this task individually.**
- **(PP) – Programming Projects (40%) –** Students will work, **in a group of 3,** on 4 programming lab projects defined by the instructor. Students also need to set up the Ubuntu VM and the lab environment (Project Deliverable 0) before the programming labs begin. The aim of the projects is to understand security concepts and principles, learn about security tools, analyze, and evaluate security threats and vulnerabilities and provide solutions for them. The students need to write programs, answer questions and write reports about the project. The details will be given in documents and will be posted on Brightspace.
- **(Extra Credit for COS 430) (CP) – In Class Presentation (5%)** – Students, in a group of 2, will present a topic of the lectures in class, lead the discussions, and respond to other students' questions. **This is mandatory for graduate students (who registered as COS530) and an extra credit for COS430 students**. The topics will be given as first come, first served. **Students should write an email to the instructor by January 25th, 2024, for the topic.**
- **Attendance Policy –** Attendance is not directly mandatory in this course. The students are expected to attend the class on a regular basis, and if they cannot attend the class, they are required to check the lecture slides. All students are required to participate in discussions in class, or on COS430/530 Discord Server regularly to receive the class participation grades.
- **Note that, the total possible grade in this class is 105, which includes 5% extra credit.**

Grading Policy:

The grading scale for the final mark is as follows:

Letter Grades	Numerical Range	Letter Grades	Numerical Range
A	95 – 100	**C**	74 - 76.99
A-	90 - 94.99	**C-**	70 - 73.99
B+	87 - 89.99	**D+**	67 - 69.99
B	84 - 86.99	**D**	64 - 66.99
B-	80 - 83.99	**D-**	60 - 63.99
C+	77 - 79.99	**F**	0 - 59.99

This scale may be curved to raise student grades at the instructor's discretion.

- Submitted work is due when specified. **With the instructor's permission and only in special cases**, you may be able to submit **TWO** days late (with a penalty). For every 12 hours of late submission, 10% points will be deducted. That is, if you are late by *two full days*, the 40% points will be deducted. After 48h, your assignment, project, and reports will be marked as 0, **with no exception.**
- Every submission has to be done through Brightspace in a digital format. Submissions via email or in person will be marked as 0. If you encounter any problems with Brightspace, it is your own duty to inform the instructor **in a timely manner, before the due date**. Brightspace problems can't be used as an excuse for a late submission.

Course Schedule: The table (below) provides the initial distribution of topics discussed over the weeks in the semester. This schedule is tentative and subject to change at the instructor's discretion. All changes will be announced in class and on Brightspace. In the event of an extended disruption of normal classroom activities, the format for this course may be modified to enable its completion within its programmed time frame. In that event, you will be provided an addendum to the syllabus that will supersede this version.

Week	Class (Tu/Th)	Activity	Material
1	01/16	L0	Syllabus and Introduction
	01/18	L1	Introduction to Computer Security
2	01/23	L2	Introduction to Computer Security – **Assignment 1 (Posted)**
	01/25	L3	Authentication, Password and Access Control
	01/26	-	**Group Selection for Security Reports (Due Date)**
3	01/30	L4	Authentication, Password and Access Control
	02/01	L5	Introduction to Cryptography
	02/04	-	**Assignment 1 (Due Date)**
4	02/06	L6	Introduction to Cryptography – **Assignment 2 (Posted)**
	02/08	L7	Introduction to Cryptography – **Project Deliverable 0 (Due Date)**
	02/11	-	**Security Report 1 (Due Date)**
5	02/13	L8	Introduction to Cryptography
	02/15	L9	Software Security and Malicious Software
	02/18	-	**Project Deliverable 1 (Due Date)**
6	02/20	L10	Software Security and Malicious Software
	02/22	L11	Software Security & Web Security
	02/25	-	**Security Reports 2 (Due Date)**
7	02/27	L12	Web Security
	02/29	L13	Web Security & Database Security
	03/03	-	**Assignment 2 (Due Date)**
8	03/05	L14	Database Security – **Assignment 3 (Posted)**
	03/07	L15	Security in OS
	03/10	-	**Project Deliverable 2 (Due Date)**
9	3/11 - 15	-	Spring Break
10	03/19	L16	Security in OS
	03/21	L17	Network Security
	03/24	-	**Security Report 3 (Due Date)**
11	03/26	L18	Guest Lecture – Alec Guertin – Google – Android Security Team
	03/28	L19	Network Security
	03/31	-	**Project Deliverable 3 (Due Date)**
12	04/02	L20	Network Security
	04/04	L21	Privacy and Anonymity
	04/07	-	**Security Report 4 (Due Date)**
13	04/09	L22	Privacy and Anonymity
	04/11	L23	Privacy and Anonymity & Security Risk Management
	04/14	-	**Assignment 3 (Due Date)**
14	04/16	L24	Security Risk Management & Legal Issues and Ethics
	04/18	L25	Guest Lecture – John Poulin – Senior Security Consultant
	04/21	-	**Project Deliverable 4 (Due Date)**
15	04/23	L26	Emerging Topics – IoT and Cloud
	04/25	L27	TBD

Academic Honesty Statement:
Academic honesty is very important. It is dishonest to cheat on exams, to copy term papers, to submit papers written by another person, to fake experimental results, or to copy or reword parts of books or articles into your own papers without appropriately citing the source. Students committing or aiding in any of these violations may be given failing grades for an assignment or for an entire course, at the discretion of the instructor. In addition to any academic action taken by an instructor, these violations are also subject to action under the University of Maine Student Conduct Code. The maximum possible sanction under the student conduct code is dismissal from the University. Please see the University of Maine System's Academic Integrity Policy listed in the Board Policy Manual as Policy 314 (***Date Issued:** September 1, 2020): https://www.maine.edu/board-of-trustees/policy-manual/section-314/

COVID-19 Return:
To keep our campus safe, students are expected to comply with all University policies related to the COVID-19 pandemic. For the latest guidance, please visit https://umaine.edu/return

The website address could be, alternatively, the system one: https://www.maine.edu/together/community-guidance/students/

Students Accessibility Services Statement:
If you have a disability for which you may be requesting an accommodation, please contact Student Accessibility Services, 121 East Annex, 581.2319, as early as possible in the term. Students who have already been approved for accommodations by SAS and have a current accommodation letter should meet with me, Dr. Sepideh Ghanavati, privately as soon as possible.

Course Schedule Disclaimer (Disruption Clause):
In the event of an extended disruption of normal classroom activities (due to COVID-19 or other long-term disruptions), the format for this course may be modified to enable its completion within its programmed time frame. In that event, you will be provided an addendum to the syllabus that will supersede this version.

UMaine Student Code of Conduct:
All students are expected to conform to the UMaine Student Code of Conduct.

Classroom Civility:
Civility should be conveyed to all others through courteous expression, politeness, esteem and regard for others, and a general respect for others, regardless of differences from self.

Inclusive and Non-Sexist Language:
The University of Maine, as an equal opportunity educational institution, is committed to both academic freedom and the fair treatment of all individuals. It therefore discourages the use of sexist language. Language that reinforces sexism can arise from imprecise word choices that may be interpreted as biased, discriminatory, or demeaning even if they are not intended to be. Accordingly, all University communications, whether delivered orally or in writing, shall be free of sexist language.

This policy shall apply to all future University publications, whether produced through Public Affairs or elsewhere, that are intended for distribution to students, parents, faculty, staff, or other people interested in the University of Maine. University publications shall include, but not necessarily be limited to: University printing office publications; promotional materials distributed by all units of the University both academic and nonacademic; and policy booklets prepared for students and faculty. Inventory on hand of existing publications may be used until exhausted or a publication is revised.

Each member of the University community is urged to be sensitive to the impact of language and to make a personal commitment to eliminate sexist language. Supervisory personnel have a particular responsibility to discuss this policy with faculty and staff and to make available to them guidelines on nonsexist language. Guidelines of the American Psychological Association on the use of nonsexist language provide direction and are recommended because they are brief and list examples, but others may be used. Consult the Communications and Marketing Department or Women's Gender and Sexuality Studies Program for alternatives (https://umaine.edu/womensgenderandsexualitystudies/) .

Observance of Religious Holidays/Events:
The University of Maine recognizes that when students are observing significant religious holidays, some may be unable to attend classes or labs, study, take tests, or work on other assignments. If they provide adequate notice (at least one week and longer if at all possible), these students are allowed to make up course requirements as long as this effort does not create an unreasonable burden upon the instructor, department or University. At the discretion of the instructor, such coursework could be due before or after the examination or assignment. No adverse or prejudicial effects shall result to a student's grade for the examination, study, or course requirement on the day of religious observance. The student shall not be marked absent from the class due to observing a significant religious holiday. In the case of an internship or clinical, students should refer to the applicable policy in place by the employer or site.

Sexual Discrimination Reporting:
The University of Maine is committed to making campus a safe place for students. Because of this commitment, if you tell a teacher about an experience of **sexual assault, sexual harassment, stalking, relationship abuse (dating violence and domestic violence), sexual misconduct or any form of gender discrimination** involving members of the campus, **your teacher is required to report** this information to Title IX Student Services or the Office of Equal Opportunity.

If you want to talk in confidence to someone about an experience of sexual discrimination, please contact these resources:

For *confidential resources on campus*: **Counseling Center: 207-581-1392** or **Cutler Health Center: at 207-581-4000**.

For *confidential resources off campus*: **Rape Response Services:** 1-800-871-7741 or **Partners for Peace**: 1-800-863-9909.

Other resources: The resources listed below can offer support but may have to report the incident to others who can help:

For *support services on campus*: **Title IX Student Services: 207-581-1406**, **Office of Community Standards: 207-581-1409**, **University of Maine Police: 207-581-4040 or 911**. Or see the OSAVP website for a complete list of services.

Copyright Notice for Materials Accessible through this Website
Most materials accessible through this site, such as linked articles, should be assumed to be copyright protected.
1. Unless the "fair use" provisions of copyright law apply or language is contained in a work permitting its use, permission should be obtained from the copyright holder for copying the work.

2. Use of the instructor prepared web pages and the slides affiliated with each lecture on the syllabus may be assumed to be controlled by the University of Maine System Broad Application Copyleft License (proposed, current, or future) or through a similar license that may be posted at the bottom of each web page.
3. All class videos (lectures) should be assumed to be copyright protected in accordance with the University of Maine System Statement of Policy Governing Patents and Copyrights.

Contingency Plans in the Event of an Epidemic:
In the event of influenza or similar epidemic that precludes the ability to meet in face-to-face sessions, assume that the instructor will either (1) host the course on our usual zoom URL for the class at the normal time and everyone will participate at a distance or (2) record a video of the lecture I would have otherwise presented in person and post it for viewing by downloading from the syllabus and/or from a web streaming video site (example: recorded on zoom or recorded and then posted on the Spatial Information Science and Engineering YouTube Channel). All other reading and module assignments should proceed as usual. If you yourself become sick, simply inform the instructor, and the instructor will arrange appropriate extensions based on your particular circumstances.