University of Maine
School of Computing and Information Science

Course Name: Introduction to Cybersecurity **Number:** COS430 **Semester:** Spring 2019
Class room: Shibles Hall 202 **Class Hours:** 2:00 – 2:50 PM **(**MWF)

Instructor: Sepideh Ghanavati **Office:** Boardman Hall234 **Email:** sepideh.ghanavati@maine.edu
Instructor Office Hours: Wednesdays 3:00 – 4:30 or by appointment

TA: Sanonda Gupta **TA-Office:** TBA **TA-Email:** TBA
TA-Office Hours: TBA

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 – 5th Edition – Charles P. Pfleeger, Shari Lawrence Pfleeger, Jonathan Margulies – 2016.
Chapters to read will be mentioned every week, under the mandatory part.

Reading Materials (optional): The optional/complementary textbooks of the course is:
Computer Security: Principles and Practice – 4th Edition – William Stallings, Lawrie Brown – 2017.

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. Communication and Network Security
5. Security Operations
6. Risk and Incident Management
7. Legal Issues, Ethics and Privacy
8. Emerging Technologies

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 in information security, including security policies, security models, and security mechanisms.
- Explain concepts related to applied cryptography, including plain-text, 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, 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, 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, TP, P
2. Analyze and evaluate components and systems with respect to security principles and practices.	1	D, A, TP, P
3. Perform risk and threat assessment.	1	D, A, TP, P
4. Understand legal, regulatory, privacy and ethical topics.	4	D, A, TP, P
5. Working Effectively in teams.	5	TP

Activities and Evaluation:
Students' performance will be evaluated based on class participation/discussions, assignments and a project.

- **Lectures** – There will be 150 minutes of lectures every week, Monday, Wednesday and Friday, in which students will learn about topics in cybersecurity.
- **Readings** – Students will be assigned readings from the course textbook or academic papers to learn techniques, principles and concepts related to cybersecurity.
- **(D) – Class Participation and Discussion Forum (10%)** – Students reflect on reading materials, discussions and exercises in the class as well as on the discussion forum. This is an **individual** assessment. We discuss different subjects related to the course in class and the participation is required. There will also be in class exercises that students are required to participate and provide solutions on. In addition, students must assess and give feedback on other students' projects.
- **(A) – Assignments (40%)** – Students have 4 take-home assignments during the semester whereby students apply methods taught in class to sample problems. All assignments are **individual** efforts.
- **(TP) – Term Project (50%) –** Students will work in **a group of 4 or 5 students** on a project from the topics given by the instructor. The detail of the topics must be approved by the instructor by the deadline specified below. The aim of these projects is to understand security concepts and principles, analyze and evaluate security threats and vulnerabilities and provide solutions for them. The students

will need to write a report for the project and present their result in class. The detail of the project is given in another document.

- **P – Optional Presentation (5%)** – Students have an opportunity to give 20 minutes in class presentation related to the topics of the lectures. The presentations should be approved by the instructor 1 to 2 weeks prior to the date. Students can present in the group of maximum 3. This is an optional effort and it counts as bonus marks.
- **Attendance Policy** – Students are allowed to have 5 free absences (whether excused or not). More than 5 absences will be penalized. The 6th missed class will have 2 marks (2%) deduction of the overall final grade. After that, each absence, except on the days of students' presentations, will count as 1% deduction of the overall final grade. For example, if your total mark at the end of the semester is 90% and you have missed 6 classes, your final mark will be 88%. On the days of students' presentations, each absence, unless having a valid excuse, will have 3% deduction of the overall final grade, regardless of having any free absence left. If a student comes late to their own presentation, the presentation's mark will be deducted by 20% for that specific student. Note that, if the students show up more than 10 minutes later than the start of the class (i.e. after 2:10pm), they will also be marked as absent. More details are given in the section, Class Attendance, below.
- **Note: The total of possible marks in this class is 105 which includes 5% bonus marks.**

Grading Policy:
The grading scale for the final mark is as follows:

Letter Grades	Numerical Range
A+	97 – 100
A	94 - 96.99
A-	90 - 93.99
B+	87 - 89.99
B	84 - 86.99
B-	80 - 83.99
C+	77 - 79.99
C	74 - 76.99
C-	70 - 73.99
D+	67 - 69.99
D	64 - 66.99
D-	60 - 63.99
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, you may be able to submit 1-3 days late (with a penalty). For every 12 hours of late submission, 5% marks will be deducted. That is, if you are late by 3 full days, 30% mark will be deducted. After the 3rd full day, your assignment, project and reports will be marked as 0, **with no exceptions.**
- Every submission has to be done through Blackboard in a digital format. Submissions via email or in person will be marked as 0. If you encounter any problems with Blackboard, it is your own duty to inform the instructor **in a timely manner, before the due date**. Blackboard problems can't be used as an excuse for 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 during the semester at the instruction discretion**. All changes will be announced in class or on the course website (Blackboard). Students are responsible for making sure they are informed about announcements.

Week	Class (MWF)	Activity	Material
1	01/23	L0	Syllabus and Introduction
	0/125	L1	Introduction to Computer Security
2	01/28	L2	Introduction to Computer Security – **Assignment 1 (Posted)**
	01/30	L3	Authentication, Password and Access Control
	02/01	L4	Authentication, Password and Access Control **– Project Topic (Due Date)**
3	02/04	L5	Introduction to Cryptography
	02/06	L6	Introduction to Cryptography
	02/08	L7	In Class Practice
4	02/11	L8	More advanced Cryptography **– Project Deliverable 0 (Due Date)**
	02/13	L9	More advanced Cryptography
	02/15	L10	Software Security and Malicious Software
5	02/18	-	No Class – President Day
	02/20	L11	Software Security and Malicious Software
	02/22	L12	In Class Practice
	02/23	-	**Assignment 1 (Due Date)**
6	02/25	L13	Software Security and Malicious Software
	02/27	L14	Web-User Security – **Assignment 2 (Posted)**
	03/01	L15	Web-User Security **– Project Deliverable 1 (Due Date)**
7	03/04	L16	Security in OS
	03/06	L17	Security in OS
	03/08	L18	In Class Practice
	03/10	-	**Assignment 2 (Due Date)**
8	03/11	L19	Guest Lecture – Network Security – Concepts – **Assignment 3 (Posted)**
	03/13	L20	Guest Lecture – Network Security – Attacks
	03/15	L21	No Class
9	03/18 03/22	-	Spring Break
10	03/25	L22	Guest Lecture – Network Security – Strategic Defenses
	03/27	L23	Guest Lecture – Network Security **– Project Deliverable 2 (Due Date)**
	03/29	L24	In Class Practice
11	04/01	L25	Database Security – **Assignment 3 (Due Date)**
	04/03	L26	Database Security – **Assignment 4 (Posted)**
	04/05	L27	Guest Lecture – Dr. Betina Tagle
12	04/08	L28	Privacy and Anonymity
	04/10	L29	Legal Issues and Ethics
	04/12	L30	Guest Lecture – John Poulin
13	04/15	L31	Security Risk Management
	04/17	L32	Emerging Topics Overview (IoT, Cloud Computing and Blockchain)
	4/18	-	**Deliverable 3 (Due Date)**
	04/19	L33	Blockchain/ Students Presentation
14	04/22	P2	Students Presentation – **Assignment 4 (Due Date)**
	04/24	P3	Students Presentation
	04/26	P4	Students Presentation
15	04/29	P5	Students Presentation
	05/01	L34	No Class – Maine Day
	05/03	L35	Placeholder
	05/04	-	**Project Deliverable 4 (Due Date)**

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.

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, 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 the campus Office of Sexual Assault & Violence Prevention 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:** 1-800-310-0000 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: **Office of Sexual Assault & Violence Prevention: 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 at http://www.umaine.edu/osavp/

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 an 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 ConnectPro 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 ConnectPro 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.

Additional References:

Recommended Readings:

[1] Ross Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley, 2008.

[2] Mathias Payer, Software Security: Principles, Policies, and Protection (SS3P), In SS3P'18: Open Textbook, 2018.

Additional Resources:

[1] Julia H. Allen, Sean Barnum, Robert J. Ellison, Gary McGraw, and Nancy Mead, Software Security Engineering: A Guide for Project Managers by. Addison-Wesley, ISBN 978-0-32-150917-8

[2] Steven Bellovin. Thinking Security: Stopping Next Year’s Hackers (Addison- Wesley Professional Computing Series). Addison-Wesley Professional, 2015.

[3] Toby Fulwiler and Alan R. Hayakawa. The Blair Handbook: 2009 MLA Update Edition. 5th. Longman, 2009. ISBN: 978-0205735594.

[4] David Kahn, The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet. Scribner, 1996.

[5] Steven Levy, Crypto: How the Code Rebels Beat the Government Saving Privacy in the Digital Age. Penguin Press Science, 2001. ISBN: 978-0140244328.

[6] Gary McGraw, Software Security: Building Security In. Addison-Wesley Professional, 2006.

[7] Bruce Schneier, Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. W. W. Norton, 2015.

[8] Bruce Schneier, Secrets and Lies: Digital Security in a Networked World, Wiley, 2004.

[9] Simon Singh, The Code Book. Anchor, 2000. ISBN: 978-0385495325.

[10] Edward Skoudis and Tom Liston, Counter Hack Reloaded: A Step-by-Step Guide to Computer Attacks and Effective Defenses (2nd Edition). Prentice Hall, 2006.

[11] Clifford Stoll, The Cuckoo’s Egg: Tracking a Spy Through the Maze of Computer Espionage. Pocket Books, 2005.

[12] William Strunk Jr. and E. B. White, The Elements of Style. 4th. Longman, 1999. ISBN: 978-0205309023.

[13] Dafydd Stuttard & Marcus Pinto, The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws, Wiley, September 2011. ISBN: 1118026470 / 978-1118026472.

[14] William Zinsser, On Writing Well: The Classic Guide to Writing Nonfiction. 30th Anniversary Edition. Harper Perennial, 2006. ISBN: 978-0060891541.